PATENT ABSTRACTS
Korean Application No: 1998-33266

The published Korean patent application 1998-33266(publication date:1998.07.25, referred to as "cited reference") discloses a method of decrypting data and a method of restricting the use of software by a limited value(permissible expiry date, etc.) in which, in delivering the data from a server to a client through a public communication network, the server restores the encoding key with a volume ID and restores the public key of the client by the volume ID and publication number. After the server encrypts the encryption key into dual-encrypted data by using a pseudo-random number and the public key and transmits that to the client, the client decrypts the dual-encrypted data with the secret key of the client corresponding to the public key so as to get the encryption key, and decodes the data with the encryption key.

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[6]
G06F 15/00

(11) 공개번호 특1998-033266
(43) 공개일자 1998년07월25일

(21) 출원번호	특1997-055868
(22) 출원일자	1997년10월29일
(30) 우선권주장	96-286345 1996년10월29일 일본(JP)
(71) 출원인	마쓰시타 덴키산교 (주) 모리시타 요오이치
	일본 오사카후 가도마시 오오아자 가도마 1006
(72) 발명자	우라나카 사치코
	일본 도쿄도 분쿄쿠 혼코마고메 3-13-8
	키요노 마사키
	일본 가나가와켄 가마쿠라시 가지와라 4-3-4 비-301
(74) 대리인	이병호, 최달용

심사청구 : 있음

(54) 사용자가 사용항목으로 분포된 애플리케이션 패키지를 사용하는 것을 허용하기 위한 시스템 및 애플리케이션 패키지

요약

인증된 사용자만이 소정의 동작 중 하나로, 예를 들면 무료 플레이 모드, 유료 모드, 제한-부착 플레이 모드 등으로 분포된 애플리케이션 패키지에 포함되는 원하는 애플리케이션을 플레이하는 것을 허용하기 위한 시스템이 제공된다. 시스템은 통신 네트워크를 통해 클라이언트와 연결되는 서버(server)의 제어하에서 애플리케이션을 플레이하는 클라이언트를 구비한다. 애플리케이션 패키지(볼륨(volume)는 볼륨의 애플리케이션 및 볼륨에 지정된 모드 코드를 포함하는 분포 설명자를 포함한다. 분포 설명자의 데이터는 볼륨의 분포시 결정되어 설명자에 저장된다. 이러한 특성은 시스템을 탄력적으로 만든다. 또한, 서버와 통신하지 않고 동작가능한 시스템이 설명된다.

대표도

도1

명세서

도면의 간단한 설명

도 1은 본 발명의 제 1 실시예에 따라 사용자가 더 높은 보안성을 갖는 패키지(package)의 사용 항목으로 분포된 애플리케이션 패키지를 사용하는 것을 허용하는 시스템의 배열을 도시한 블록도.

도 2는 본 발명의 시스템에서 사용되는 DVD상에 기록된 애플리케이션(또는 유료 정보) 패키지의 모범적인 구조를 도시하는 도면.

도 3 및 도 4는 각각 볼륨(volume) 설명자(22) 및 분포 설명자(23)의 모범적인 데이터 구조를 상세한 형태로 도시하는 도면.

도 5는 본 발명의 원리에 따라 DVD상에 기록된 애플리케이션을 플레이하는 볼륨 제어 프로그램의 흐름도.

도 6A는 도 1에 도시된 서버(server)에 저장되는 볼륨 데이터 도표의 모범적인 구조를 도시하는 도면.

도 6B는 서버(8)에 저장되는 애플리케이션 데이터 도표의 모범적인 구조를 도시하는 도면.

도 7은 클라이언트(2)의 EEPROM(103)에 저장되는 서버 도표(75)의 구조를 도시하는 도면.

도 8A 및 도 8B는 처리(650), (700), 및 (800)의 시작부에서 각각 클라이언트(2) 및 서버(8)에 의해 서로 작용하여 실행되는 초기화 루틴의 흐름도.

도 9는 도 5의 단계(650)로 도시된 무료 플레이 처리의 절차를 도시하는 것으로, 두 개의 흐름선으로 인접한 블록을 연결시키는 것은 각 블록이 클라이언트 및 연관된 서버에 의해 서로 작용하여 실행됨을 나타내는 흐름도.

도 10A 및 도 10B는 서로 작용하여 실행되는 모범적인 기대 플레이 시간 통보 루틴으로 형성된 절차를 결합하여 도시하는 흐름도.

도 11A 및 도 11B는 기간의 시간을 정하고 플레이 이후에 시간 지정된 플레이 기간을 디스플레이하면서 애플리케이션을 디스플레이하도록 서로 작용하여 실행되는 모범적인 시간 지정 플레이 및 미터(meter) 사

용 보고 루틴으로 형성된 절차를 결합하여 도시하는 흐름도.

도 12A 및 도 12B는 기간의 시간을 정하면서 애플리케이션을 플레이하도록 서로 작용하여 실행되는 모범적인 시간 지정 애플리케이션-플레이 서브루틴으로 형성된 절차를 결합하여 도시하는 흐름도.

도 13A 및 13B는 플레이 시간의 시간 지정이 클라이언트내의 타이머로 이루어지도록 서로 작용하여 실행되는 다른 방법의 시간 지정 애플리케이션-플레이 서브루틴으로 형성된 절차를 결합하여 도시하는 흐름도.

도 14는 각각 도 12A 및 도 13A의 단계 (612) 및 (622)에서 호출되고, 제어기(100)에 의해 실행되는 모범적인 애플리케이션 플레이 서브루틴의 흐름도.

도 15는 도 5의 단계(700)로 도시된 유료 플레이 처리(700)의 절차를 도시하는 흐름도.

도 16A 및 16B는 서로 작용하여 실행되는 모범적이 기대 청구 통보 루틴으로 형성된 절차를 결합하여 도시하는 흐름도.

도 17A 및 17B는 도 15의 블록(650)에서 서로 작용하여 실행되는 루틴으로 형성된 절차를 결합하여 도시하는 흐름도.

도 18A 및 도 18B는 플레이를 실행하면서 기간의 시간을 정하고 플레이 이후에 요금 청구 및 총 청구량을 디스플레이하도록 서로 작용하여 실행되는 절차를 결합하여 도시하는 흐름도.

도 19는 도 5의 동작 블록(800)에서 클라이언트(2) 및 서버(8)에 의해 서로 작용하여 실행되는 절차를 도시하고, 두 개의 흐름선을 연결된 블록은 두 개의 소자(2) 및 (8)에 의해 블록 동작이 행해짐을 나타내는 흐름도.

도 20A 및 20B는 각각 서버에 저장되는 키-암호키 도표 및 사용자 공증키를 도시하는 도면.

도 20C는 서버(8)로부터 애플리케이션 암호키(Kv)를 구하는 처리 과정의 흐름도.

도 21은 본 발명에 따른 모범적인 IC 카드 IF 내에 조립된 해독기의 블록도.

도 22는 도 20C의 암호화시스템을 이용한 시스템(1)에서 도 21의 Kv 디코더(126)를 대신해 사용되는 Kv 디코더를 도시하는 도면.

도 23은 사용 항목(terms-of-use, TOU) 코드와 대응하는 제한값의 의미를 설명하는 도면.

도 24는 본 발명의 제 2 실시예에 따라 서버와 통신하지 않고 패키지의 사용 항목으로 분포된 애플리케이션 패키지를 플레이하기 위한 시스템의 배열을 도시하는 블록도.

도 25는 도 24에 도시된 제어기(100a)에 의해 실행되는 모범적인 제어 프로그램을 도시하는 흐름도.

도 26 및 도 27은 도 25의 단계(650a)에서 도시된 무료 플레이 모드의 동작을 각각 상세한 형태와 더 상세한 형태로 도시하는 흐름도.

도 28은 도 25의 단계(800a)에서 도시된 제한 부착 플레이 모드의 동작을 도시하는 흐름도.

도면의 주요부분에 대한 부호의 설명

1 : 시스템(1)2 : DVD 플레이어

3 : DVD4 : 통신 네트워크

6 : 제공자7 : 서버

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 일반적으로 보안 시스템에 관한 것으로, 특히 인증된 사용자가 공급된 유료 정보의 사용을 청구 및 제어하면서 패키지(package) 또는 전송 매체를 통해 공급된 유료 정보를 사용하도록 허용하기 위한 방법 및 시스템에 관한 것이다.

다양한 유료 정보 프로그램을 제공하는 정보 제공자에 의해 제공자는 음악, 영화, 게임 등과 같은 유료 정보를 사용하기 위해서는 사용자가 일반적으로 두 단계를 취해야 한다. 제 1 단계(구입 단계)에서, 사용자는 원하는 프로그램이 기록된 FD(floppy disc), 광학 디스크(예를 들면, CD-ROM(compact disc read only memory) 및 DVD(digital versatile disc or video disc))등과 같은 패키지 매체를 구매하거나(오프-라인(off-line) 분포나 구입) 소정의 절차를 통해 정보 제공자의 서버(server) 컴퓨터로부터 원하는 프로그램을 다운 로드(down load)함으로써(온-라인(on-line) 분포나 구입) 정보 제공자 중 하나로부터 원하는 프로그램을 구입한다. 온-라인 구입의 경우에는 사용자가 프로그램을 구입하면서 플레이하거나(즉, 두 단계가 평행하게 실행되거나) 제 1 단계에서 프로그램을 구입하면서 저장하고 나중에 제 2 단계(또는 사용 단계)로서 프로그램을 실행시킨다. 오프-라인 구입의 경우에서는 제 2 단계에서 사용자가 구입된 기록 매체를 적절한 장치로 로드시키고 직접 프로그램을 플레이(또는 실행)하거나, 일단 프로그램을 장치의 메모리에 저장하고 이어서 프로그램을 플레이 한다.

일본 특허 비심사 공개 제 1995-295674(1995)호는 제 2 또는 사용 단계에서 CD-ROM을 사용하는 보안 시스템을 설명한다. 이 시스템에서, 사용자는 센터 공증키(center public key)로 암호화되어 정보에 포함된

원하는 프로그램의 코드와 사용자 발생 키를 정보 제공자에 전달하고, 사용자 발생 키로 암호화되어 정보 제공자에 의해 전달된 암호화 키로 정보를 해독함으로서 톨 센터(toll center)의 공중키(센터 공중키)와 함께 CD-ROM에 기록된 암호화 정보를 사용할 수 있다. 그러나, 사용자의 신원이 확인되지 않아, 다른 사람의 CD-ROM을 구입한 불성실 사용자가 이를 사용하는 것을 허용하게 된다. 또한, 센터 공중키는 CD-ROM에서 암호화된 정보와 함께 인쇄된다. 이는 센터 공중키를 변화시키는 것을 어렵게 만든다. 또한, 이로 인하여 다른 센터 공중키를 사용하기를 원하는 다른 제공자가 CD-ROM을 인쇄할 때 CD-ROM 제작자에게 다른 마스터(또는 날인)를 사용하도록 강요하게 된다.

일본 특허 비심사 공개 제 1995-288519(1995) 호는 제 1 및 제 2 단계 모두에서 사용되는 보안 시스템을 설명한다. 그러나, 이 시스템은 유료 정보가 온-라인으로 분포된 시스템에만 적용가능하다.

일본 특허 비심사 공개 제 1996-54951(1996) 호는 사용되는 소프트웨어량이 주시되고, 또한 그 양이 소정의 양을 넘으면 사용자에 의한 소프트웨어 사용이 방해되는 시스템을 설명한다. 소프트웨어 사용을 방해하기 위해서는 전용 소프트웨어가 필요하므로, 이러한 시스템은 단지 온-라인 분포 시스템내의 서버에서 사용되기에 적합하다.

또한, 사용자가 시도 주기를 정의하는 데이터로 분포된 소프트웨어를 시도 주기 동안에만 사용하는 것을 허용하는 시스템이 있다. 이러한 시스템에서는 불성실 사용자가 소프트웨어를 다시 설치하거나 지난 시간에 대해 사용자 시스템 클럭을 설정함으로써 소프트웨어를 재사용가능하게 만들 수 있다.

종래 기술에는 이러한 프로그램 및 다른 프로그램이 있다. 본 발명의 목적은 인증된 사용자(정보 제공자로부터 온-라인 또는 오프-라인으로 유료 정보를 합법적으로 구입한 사용자)만이 각 사용 시간에 대해 청구되는 제한없이, 또는 유료 정보의 종류에 따른 사용자 제한 요소(예를 들면, 사용량, 구매 날짜가 현재 날짜 이래로 경과된 날)의 허용범위 내에서 유료 정보를 사용하는 것을 허용하는 시스템을 제공하는 것이다.

본 발명이 이루고자 하는 기술적 과제

본 발명의 원리에 따라, 유료 정보나 애플리케이션 패키지는 매체 제목 및 매체 코드와 같은 최소한 제어 정보와 함께 패키지(또는 기록) 매체나 전송 매체를 통해 분포되는 것으로 가정된다. 그러나, 설명되는 실시예는 주로 DVD에 의해 분포되고 그에 기록된 유료 정보와 연관되어 설명된다.

유료 정보의 종류에 대해, 유료 정보는 사용자에 의해 구입될 때 키로 암호화되어 DVD에 기록된다. 플레이될 분포 유료 정보가 제한없이 플레이가능한 종류이면, 유료 정보 처리는 다음의 방법으로 이루어진다. DVD를 판매할 때 키가 기록되었던 DVD로부터 먼저 키가 사용자 공중키-암호화 형태로 구해진다. IC 카드에 기록된 사용자 비밀키로 사용자 공중키-암호화 키가 해독키로서 해독된다. 또한, 암호화 유료 정보가 해독키로 해독되어 소모(즉, 플레이 또는 실행)된다. 사용자 공중키-암호화 키는 클라이언트에 서비스를 제공하는 서버(장치)로부터 온-라인으로 구해진다.

플레이될 분포 유료 정보가 사용 감지 청구형이면, 사용자는 정보를 사용할 때마다 청구된다. 이러한 경우에는 유료 정보를 처리하기 전에, 클라이언트가 사용자의 신용카드 번호를 이중 암호화하여 정보 제공자의 요금 서버중 하나에 전달하고, 서버가 정보와 연관되어 사용된 양(예를 들면, 플레이 시간이나 기간)을 볼륨 데이터 도표(volum data table)에서 총량(소프트웨어 미터(meter)) 필드(field)의 값에 더하여, 업데이트된 총량의 값을 클라이언트에게 전달하고, 또한 클라이언트가 업데이트된 총량을 디스플레이한다. 이어서, 클라이언트는 유료 정보처리를 시작한다.

플레이될 분포 유료 정보가 제한 접속형이면, 즉 정보의 사용이 정보 소모에 관한 특정한 제한 요소의 허용범위에 의해 제한되어야 하면, 클라이언트는 사용자 제한 요소가 미리 설정된 제한내에 있는 경우에만 유료 정보를 소모하도록 허용된다. 이러한 종류의 유료 정보인 경우에는 유료 정보를 처리하기 전에, 클라이언트가 DVD에 기록된 사용자 지정 애플리케이션의 식별(ID) 코드를 서버에 전달하고, ID 코드를 수신할 때 서버는 사용자 지정 애플리케이션과 연관된 사용자 제한 요소가 미리 설정된 제한내에 있는가를 시험하고, 그렇지 않으면, 서버는 시험 결과를 서버에 알리고, 클라이언트는 시험결과를 디스플레이하고, 시험이 성공적이었으면, 서버는 사용자 제한 요소의 미터(또는 합계)를 업데이터하고 업데이트된 값을 클라이언트에 전달하고, 또한 업데이트된 값의 수신에 응답해 클라이언트는 업데이트된 값을 디스플레이한다. 이어서, 클라이언트는 유료 정보 처리를 시작한다.

본 발명의 구성 및 작용

다음의 설명을 더 잘 이해하기 위해, 사용되는 일부 용어를 정의할 필요가 있다.

정보 제공자에 의해 제공되는 유료 정보는 오프-라인(off-line)(오프-라인 분포) 또는 온-라인(on-line)(온-라인 분포)으로 공급될 수 있다. 오프-라인 공급에서, 유료 정보는 패키지 매체나 기록 매체에 기록되고, 제공자의 판매 네트워크를 통해 분포된다. 즉, 판매 네트워크내의 상점에서 판매된다. 패키지 매체는 다양한 종류의 자기 디스크, 다양한 광학 메모리 디스크(예를 들면, CD, CD-ROM, DVD), 또한 자기 테이프 및 카트리지와 같은 모든 종류의 휴대용 기록 매체를 포함한다. 온-라인 분포에서, 유료 정보는 전송 매체를 통해 제공자 및 제공자와 정렬된 분포자의 서비스 지점에서의 서버로부터 유료 정보를 요구한 사용자의 클라이언트 장치(예를 들면, PC(personal computer))로 전송되어, 클라이언트(장치)의 기록 매체에 저장된다. 전송 매체는 서버와 클라이언트 장치 사이의 데이터 통신을 허용하는 통신 채널을 포함한다. 패키지 매체와 전송 매체는 이후 총괄적으로 분포 매체라 칭하여 진다.

유료 정보는 각각 구별없이 애플리케이션(application)이라 칭하여지는 음악, 영화, 게임 등과 같은 임의의 종류의 소프트웨어가 될 수 있다. 유료 정보의 분포 유닛은 유료 정보 패키지(charged information package) 또는 애플리케이션 패키지라 칭하여 진다. 애플리케이션 패키지에는 하나 이상의 애플리케이션이 포함된다.

본 발명은 사용자가 더 높은 보안성을 갖춘 패키지를 사용하는 항목으로 분포된 애플리케이션 패키지를

사용하는 것을 허용하기 위한 시스템에 관한 것이다.

[실시예 1]

간략화하기 위해, 제 1 실시예에서는 패키지 매체, 특히 DVD가 분포 매체로 사용되는 것으로 설명된다.

도 1은 본 발명의 제 1 실시예에 따라, 더 높은 보안성을 갖춘 DVD를 사용하는 항목으로 사용자가 DVD에 기록된 애플리케이션을 사용하는 것을 허용하기 위한 시스템의 배열을 도시하는 블록도이다. 도 1에서, 시스템(1)은 DVD(3)를 플레이하는 클라이언트 또는 DVD 플레이어(2), 통신 네트워크(4), 및 DVD(3)의 애플리케이션 패키지를 제공하는 제공자(6)의 툴 센터에 있는 서버(8)를 구비한다.

도 2는 본 발명의 시스템(1)에서 사용되는 DVD(3)에 기록된 애플리케이션(또는 유료 정보) 패키지(20)의 모범적인 구조를 도시하는 도면이다. 도 2에서, 애플리케이션 패키지(20)는 적어도 하나의 애플리케이션(21), 애플리케이션 패키지(20)에 관한 데이터를 포함하는 볼륨(또는 패키지) 설명자(22), 및 DVD(3)의 처리 이후에 예를 들면, 분포나 판매시 주로 결정되는 데이터를 포함하는 분포 설명자(23)를 구비한다. (볼륨 설명자(22) 및 분포 설명자(23)는 볼륨(20)의 볼륨 제어 데이터를 구성한다.) 본 실시예에서는 서버(8)와 결합되어 애플리케이션 패키지(20)의 사용을 제어하는 볼륨(또는 패키지) 제어 프로그램이 애플리케이션 패키지(20)에 포함되어 분포되는 것으로 가정된다. 그래서, 애플리케이션 패키지(20)는 또한 패키지(20) 사용 항목에 적합한 패키지 제어 프로그램(24)을 구비한다. 애플리케이션(21), 볼륨 설명자(22), 및 패키지(또는 볼륨) 제어 프로그램(245)은 DVD(3)를 제작할 때 DVD(3)의 데이터 영역에 기록되고, 분포 설명자(23)는 예를 들면, DVD(3)의 판매시 버스트(burst) 절단 영역에 기록된다.

도 3 및 도 4는 각각 볼륨 설명자(22)와 분포 설명자(23)의 모범적인 데이터 구조를 상세한 형태로 도시한 도면이다. 도 3에서, 볼륨 설명자(22)는 적어도 패키지나 볼륨(20)이 단 하나의 애플리케이션만 포함하면 애플리케이션 식별자와 같고 애플리케이션 패키지(20)의 제목으로 사용되는 볼륨 식별자(VIDv)(25)와, 제공자 식별자(26)와, 추후 기술된 바와 같이 볼륨 만기 데이터 및 시간의 결정되는 기본점으로 사용될 수 있는 볼륨 생성 날짜 및 시간(27)과, 또한 볼륨(20)이 이용가능한 날짜 및 시간을 나타내는 볼륨 유효 날짜 및 시간(28)을 포함한다. 볼륨(20)이 하나 이상의 애플리케이션을 포함하면, 볼륨 설명자(22)는 애플리케이션 식별자(AIDa)(29)를 더 포함한다.

도 4에서, 분포 설명자(23)는 분포 순서로 동일한 볼륨 식별자(볼륨 ID 또는 제목)(VIDv)의 각 분포 애플리케이션 패키지에 주어진 일련 번호를 포함하는 볼륨 발행 번호(NOv-i)(30)와, 제공자(6)의 툴 센터에서 서버(6)에 의해 데이터가 주어지는 서버 공중키(PKs)(31)와, PKu(사용자 공중키)-암호화 애플리케이션-암호화키(Kv)(32) 및 판매 날짜와 시간(33)의 필드를 구비한다. 키 PKs(31) 필드는 패키지(20)내의 각 애플리케이션(21)을 암호화하는데 사용되고 합법적으로 패키지(20)를 구입한 사용자의 사용자 공중키(PKu)로 암호화된 키를 포함한다. 적절한 데이터는 패키지(20)의 분포시, 즉 본 실시예에서는 DVD(3)의 판매시(34)를 통해 모든 필드(30)에 기록된다.

분포 설명자(23)는 또한 사용 항목 코드(모드 코드) + 볼륨에 대한 제한값의 필드(34)(볼륨 제한값 필드)와, 각 애플리케이션 ID(29)에서 사용 항목 코드 + 애플리케이션 ID(29)에 대한 제한값의 필드(35)(애플리케이션 제한값 필드)를 포함한다. 사용 항목이 볼륨(20)에만 설정되면, 필드(35)는 필요없다. 사용 항목이 각 애플리케이션에 설정되면, 필드는 빈 상태가 된다.

도 23은 사용 항목(terms-of-use, TOU) 코드의 의미와 대응하는 제한값을 설명하는 도면이다. 도 23에서, 사용 항목 코드는 예를 들면 1 바이트의 길이가 될 수 있다. TOU 코드의 더 높은 디지트(X)는 도표 36에 도시된 바와 같이 사용 항목이 적용되는 타겟을 나타낸다. 즉, 0, 1, 2, ..., 의 더 높은 디지트 이러한 디지트로 시작되는 TOU 코드가 전체적인 볼륨, 애플리케이션 1, 애플리케이션 2 등에 관한 것임을 나타낸다. 상술된 사용 항목 코드의 하위 디지트(Y)는 코드가 설정된 애플리케이션(21)이나 패키지(20)의 사용 항목이 도 23의 도표 37에 도시된 바와 같이 대응하는 제한값으로 직접 이어짐을 나타낸다. 특히, 00H의 사용 항목 코드(또는 TOU 코드)는 예를 들면, 볼륨(20)이 분포 이후에 자유롭게 사용될 수 있음을 의미한다. 값 '31H'는 예를 들면, TOU 코드가 설정된 애플리케이션(3)이 플레이 기간의 단위당 지불되어 사용될 수 있음을 나타낸다. 2H 또는 그 이상의 하위 디지트는 TOU 코드가 설정된 애플리케이션이나 볼륨(20)이 대응하는 제한값에 이를 때까지 자유롭게 사용될 수 있고 그 이상의 사용을 가능하지 않게 함을 의미한다. 도표로부터 알 수 있는 바와 같이, 하위 디지트가 2H 내지 5H인 TOU 코드에 의해 결정된 사용자 제한 요소는 각각 현재 날짜 및 시간, 만기 날짜 및 시간, 사용 주기량, 및 억세스 카운트이다.

분포 설명자(23)의 데이터는 상술한 바와 같이 설정될 수 있으므로, 이는 제공자 및 사용자 모두에게 종래 시스템이 제공할 수 있는 것보다 더 많은 탄력성을 제공한다.

다시 도 1에서, DVD 플레이어(2)는 전체적인 DVD 플레이어(2)를 제어하는 제어기(100)와, 제어기(100)내에 포함되는 도시되지 않은 CPU(central processing unit), 도시되지 않은 ROM(read-only memory), RAM(random access memory)(101), 및 EEPROM(electrically erasable programmable ROM)(103)과 연결된 데이터 버스(102)와, 키보드, 음성 인식 장치, 마우스, 원격 제어기 등과 같은 입력 장치를 포함하는 휴먼(human) 인터페이스(IF)(110)와, ID 카드(5)에서 버스(102)를 ROM(도시되지 않은)과 연결시키는 IC 카드 인터페이스(IF)(120)와, DVD(3)에 기록된 데이터를 판독하고 판독된 데이터를 복조 및 에러 정정하는 DVD 드라이버(130)와, MPEG 2 비트열을 수신하고 비디오 및 오디오 출력 신호를 출력하는 비디오 및 오디오 출력 IF(140)와, 디스플레이 장치(146)와, 스피커(148) 및 공중 통신 네트워크(4)를 통해 통신하는 통신 IF(150)를 구비한다. IC 카드(5)는 DVD(3)의 버스트 절단 영역에 기록된 분포 설명자(23)의 필드(32)에 포함되는 PKu-암호화 AP-암호화 키(Kv)와 연관되어 설명된 사용자 공중키(PKu)에 대응하는 사용자 비밀키(SKu)와 사용자 패스워드(PWu)를 저장한다. 비디오 및 오디오 출력 IF(140)는 MPEG 2 비디오 디코더(142)와 MPEG 2 오디오 디코더(144)를 포함한다.

DVD(3)를 구입하는데는 여러 방법이 있다. 예를 들어, 서점이나 우편 주문을 통해 DVD(3)을 사면, IC 카드(5)에 저장된 비밀키(SKu)에 대응하는 공중키(PKu)를 통보함으로써 원하는 DVD(3)의 버스트 절단 영역에 기록된 애플리케이션-암호화 키(Kv)의 PKu-암호화 버전을 가져야 한다. 서비스에 가입할 때 PKu를 통보하여야 하기 때문에, 구입자 DVD 분포 서비스의 멤버이면, 구입할 때마다 PKu를 통보하지 않고 기록된

PKu-암호화 AP-암호화 키를 갖는 DVD를 구입할 수 있다.

동작시, 사용자는 먼저 DVD 플레이어(2)의 DVD 드라이버(130)에 원하는 DVD(3)를 설정하고, 적절한 휴먼 IF(110)를 통해 DVD 플레이어(2)에 시작 명령을 전한다. 시작 명령의 수신에 응답해, 제어기(100)는 DVD 드라이버(130)를 통해 DVD(3)의 데이터 영역으로부터 볼륨 제어 프로그램(24)을 판독하여 이를 제어기(100)의 RAM(101)으로 로드시키고, 볼륨 제어 프로그램(24)을 실행한다.

도 5는 본 발명의 원리에 따라 DVD(3)에 기록된 애플리케이션(21)을 플레이하는 볼륨 제어 프로그램(24)의 흐름도이다. 도 5에서, 제어기(100)는 먼저 단계(500)에서 볼륨(20)이 단일 프로그램을 포함하는가를 보도록 AIDI 필드를 점검한다. 그렇지 않으면, 제어기(100)는 단계(502)에서 필드(29)에 애플리케이션 ID를 디스플레이하고, 애플리케이션 중 원하는 것을 선택하도록 사용자에게 촉구하고, 또한 단계(504)에서 선택을 대기한다. 단계(504)에서 애플리케이션이 선택되면, 제어기(100)는 단계(506)에서 그 애플리케이션의 애플리케이션 ID를 플레이될 애플리케이션으로 등록하고, 단계(508)로 진행하여 필드가 비어있나를 보도록 선택된 애플리케이션에 대한 사용 항목(TOU) 코드 + 제한값의 필드(35)를 점검한다. 그런 경우, 제어기(100)는 단계(510)로 진행되어 볼륨 제한 필드(34)를 판독한다.

한편, 단계(500)에서 시험 결과가 YES이면, 제어기(100)는 단계(512)에서 볼륨 ID를 플레이될 애플리케이션으로 등록하고, 단계(510)에서 볼륨 제한값(34)을 판독한다.

단계(510)가 완료되거나 단계(508)의 시험 결과가 NO이면, 제어기(100)는 단계(514)에서 사용 항목(TOU) 코드의 하위 디지트가 0인가를 보도록 TOU 코드를 점검한다. 그런 경우, 제어기(100)는 단계(650)에서 무료 애플리케이션을 플레이하고, 그렇지 않으면 단계(516)에서 TOU 코드의 하위 디지트가 1인가를 보도록 또 다른 점검을 실행한다. 그런 경우, 제어기(100)는 단계(700)에서 사용 감지 청구로 애플리케이션을 플레이하고, 그렇지 않으면(TOU 코드의 하위 디지트가 2 이상이면) 단계(800)에서 사용 제한 요소의 소프트웨어 미터가 미리 설정된 값 이하일 때만 애플리케이션을 플레이한다. 단계 또는 처리(650) 내지 (800)이 완료되면, 제어기(100)는 프로그램(24)을 종료한다. 그래서, DVD 플레이어(2)는 애플리케이션 패키지나 지정된 애플리케이션에 설정된 TOU 코드에 의해 결정되는 사용 항목에 따라 사용자에 의해 지정된 프로그램을 플레이한다.

처리 과정(650), (700) , 및 (800)은 연관된 서버(8)와 서로 작용하게 실행된다. 서버(8)는 이러한 처리를 실행하기 위해 다양한 데이터를 필요로 하고, 이러한 데이터를 도표의 형태로 저장한다.

도 6A는 서버(8)에 저장되는 볼륨 데이터 도표의 모범적인 구조를 도시하는 도면이다. 도 6A에서, 볼륨 데이터 도표(60)의 각 기록은 볼륨 ID(VIDv)와 발행 번호(NOv-i) 필드를 포함한다. VIDv와 NOv-i의 조합은 애플리케이션 패키지(20)나 DVD(3) 사용자의 사용자 ID로 동작한다. 이러한 이유로, 도표(60)는 DVD 분포 서비스 등의 가입자나 멤버에 대해 예를 들면, 멤버 ID, 이름, 주소 등을 포함하는 개인용 데이터 필드를 갖는다. 각 기록은 또한 볼륨(20)에 부착되는(또는 연관되는) 플레이 기간의 소프트웨어 미터를 분으로 포함하는 볼륨 분 미터 필드(VM-METERv-i)와, 볼륨(20)에 부착되는 소프트웨어 청구 미터를 포함하는 볼륨 청구 미터(VC-METERv-i)와, TOU 코드와 연관된 제한값을 포함하는 제한값(LVv-i)(예를 들면, 유효 날짜 및 시간, 허용가능한 만기 날짜 및 시간, 허용가능한 억세스 등)과, 제한값 미터(LV-METERv-i)와, 애플리케이션의 제목을 포함하는 애플리케이션 ID(AIDv-i-a) 필드와, AIDv-i-a의 애플리케이션에 부착되는 플레이 기간의 소프트웨어 미터를 분으로 포함하는 애플리케이션 분 미터(AM-METERv-i-a) 필드와, AIDv-i-a의 애플리케이션에 부착되는 분으로 표시된 플레이 기간의 소프트웨어 미터에 대한 애플리케이션 청구 미터(AC-METERv-i-a)와, TOU 코드와 연관되는 제한값을 포함하는 제한값(LVv-i-a) 및 제한값 미터(LV-METERv-i)를 구비한다.

도 6B는 서버(8)에 저장되는 애플리케이션 데이터 도표의 모범적인 구조를 도시하는 도면이다. 도 6B에서, 애플리케이션 데이터 도표(70)는 예를 들면, 애플리케이션 코드(ACODEn), 애플리케이션 제목(AIDn), 기간(D), 억세스당 비율(RATE/ACCESS), 억세스 카운트, 분 미터 등의 필드를 구비한다. 기간은 애플리케이션을 플레이하는데 걸리는 시간 주기이다. 억세스당 비율은 전체 애플리케이션의 플레이에 대한 청구로, 플레이하기 전에 사용자에게 예상 플레이 기간을 알리는 데 사용된다. 단위 시간당 비율은 플레이의 단위 시간에 대한 청구로, 실제로 시간이 정해진 플레이 기간에 대한 청구를 계산하는데 사용된다. 억세스 카운트 및 분 미터 필드는 애플리케이션으로의 억세스 회수와 총 플레이량을 포함하는 것으로, 본 발명에서는 필요하지 않지만 예를 들면, 기호 분석을 위한 통계적인 계산에서 사용된다.

도 7은 클라이언트(2)의 EEPROM(103)에 저장된 서버 도표(75)의 구조를 도시하는 도면이다. 도 7에서, 도표(75)의 필드는 서버 공중키(PKs), 서버 ID(SIDs), 서버 네트워크 어드레스(SADDs) 등을 포함한다. 이 도표(75)는 DVD의 버스트 절단영역에 기록된 분포 설명자(23)에 포함되는 서버 공중키(PKs)를 ID 및 네트워크 어드레스와 연관시키는데 사용된다.

무료 애플리케이션의 플레이

처리 과정 (650), (700), 및 (800)의 초기화 루틴은 모두 같다.

도 8A 및 도 8B는 처리 과정 (650), (700), 및 (800)의 시작부에서 각각 클라이언트(2) 및 서버(8)에 의해 대화식으로 실행되는 초기화 루틴(80a) 및 (80b)의 흐름도이다. 도 8A에서, 클라이언트 또는 DVD(2)의 제어기(100)는 단계(82)에서 클라이언트 또는 DVD(2)의 네트워크 어드레스(CADDc), TOU 코드 + 제한값, 볼륨 ID(VIDv), 발행 번호(NOv-i), 애플리케이션 ID(AIDv-i-a), 및 다른 데이터를 포함하는 서비스 요구를 ID가 SIDs(SIDs는 DVD(3)에 기록된 공중키를 이용함으로써 도 7의 도표(75)로부터 구해진다)인 연관되는 서버(8)에 전달되고, 단계(92)에서 커버(SIDs)(8)로부터 응답을 대기한다. 서버(SIDs)로부터 응답이 있으며, 클라이언트(2)는 그 안에 A를 포함하는 원을 통해 다음 단계로 진행된다.

한편, 도 8B에서, SIDs의 서버(8)는 단계(84)에서 클라이언트(2)으로부터 메시지, 즉 서비스 요구 및 동반 데이터를 수신하고, 순차적으로 사용되도록 소정의 위치에 데이터를 저장한다.이어서 서버(8)는 단계(86)에서 볼륨 ID 및 발행 No. 필드 각각에 VIDv 및 NOv-i를 포함하는 기록이 있는가 도표(60)를 탐색한다. 탐색이 성공적이지 않으면, 서버(8)는 단계(88)에서 도표(60)에 VIDv 및 NOv-i에 대한 기록을 부가하

고, 관련된 필드를 AIDv-i-a 및 제한값으로 채운 후 단계(90)로 진행된다. 또한, 단계(86)에서의 탐색이 성공적이면, 서버(9)는 단계(90)로 진행되고, 여기서 서버(8)는 TOU 코드값에 따라 다음에 실행되는 루틴을 선택하고 그 안에 B를 포함하는 원을 통해 선택된 루틴으로 들어간다. 이러한 경우에, TOU 코드 = x0H(x : 임의의 16진수, 마지막 위치의 문자 H는 진행되는 수가 16진수임을 나타낸다)이면, 무료 애플리케이션이 플레이되는 루틴이 선택된다. TOU 코드 = x1H이면, 사용 감지 청구로 애플리케이션을 플레이 하는 루틴이 선택된다. TOU 코드 ≥ x2H이면, 사용 제한 요소의 소프트웨어 미터가 미리 설정된 값 이하인 경우에만 애플리케이션을 플레이하는 루틴이 선택된다.

도 9는 도 5의 단계(650)로 도시된 무료 플레이 처리의 절차를 도시하는 흐름도이고, 여기서 두 흐름선으로 인접한 블록을 연결시키는 것은 각 블록이 추후 상세히 도시될 바와 같이 CADDc의 클라이언트 및 연관되는 서버(SIDs)에 의해 서로 작용하여 실행됨을 나타낸다. 도 5의 단계(514)에서 TOU 코드가 00이면, 서버(CADDc)는 도 9에 도시된 바와 같은 무료 플레이 처리(650)로 들어가고, 클라이언트 및 서버(SIDs)는 블록(660)에서 초기화 루틴(80)을 실행한다. 블록(670)에서, 예상 플레이 시간 통보 루틴이 실행된다. 즉, 지정된 애플리케이션을 플레이하기 전에 예상 플레이 시간을 디스플레이한다. 블록(680)에서, 애플리케이션 플레이 및 측정된 플레이 시간 보고 루틴이 실행된다. 루틴(80)은 도 8에서 설명되었으므로, 예상 플레이 시간 통보 루틴과 애플리케이션 플레이 및 측정된 플레이 시간 보고 루틴이 다음에 설명된다.

도 10A 및 도 10B는 각각 클라이언트(2) 및 관련 서버(8)에 의해 서로 작용하여 실행되는 모범적인 기대 플레이 시간 통보 루틴(97a) 및 (97b)으로 형성된 절차를 결합하여 도시하는 흐름도이다. 도 10B에서, 서버(8)는 단계(91)에서 이미 공지된 방법으로 도표(70)로부터 AIDv-i-A의 애플리케이션 기간(Dn)을 회복한다. 다음의 단계(92)에서, 서버(8)는 TOU 코드값에 따라 총 예상 플레이 시간량을 계산한다. 특히, TOU 코드가 0xH이면, 클라이언트는 도표(60)에서 VIDv 및 NOv-i에 의해 식별되는 기록의 VM-METERv-i 필드값과 기간(Dn)을 부가한다. TOU 코드가 axH(a : 볼륨에서 지정된 애플리케이션의 애플리케이션 번호)이면, 클라이언트는 도표(60)에서 VIDv, NOv-i, 및 AIDv-i-a에 의해 식별되는 기록의 AM-METERv-i-a 필드값과 기간(Dn)을 부가한다. 이어서, 서버(8)는 단계(93)에서 네트워크 어드레스가 CADDc인 클라이언트에게 결과를 전달하고, 처리 과정을 종료한다.

한편, 도 10A에서, 클라이언트(2)은 단계(94)에서 업데이트된 미터값이나 들어오는 메시지를 수신한다. 다음 단계(95)에서는 그 값이 총 사용량으로 디스플레이된다. 이어서, 클라이언트(2)은 처리 과정을 종료한다.

관련된 미터를 업데이트할 때, 막 설명된 도 10의 루틴에서의 소정의 기간값이 사용된다(미리 설정된 값 미터링 시스템). 이러한 배열은 주로 플레이하는데 일정한 시간이 걸리는 애플리케이션에 적합하고, 사용자가 플레이를 중단시키지 않으면 문제점을 일으키지 않는다. 이점에서, 실질적으로 미터링에서의 플레이 시간을 측정하는 것이 바람직하다(시간이 정해진 값 미터링 시스템). 그러나, 또한 미리 설정된 값 미터링 시스템은 실질적인 플레이에 앞서 사용자에게 예상 플레이 시간을 알리는데 유용함을 주목한다.

도 11A 및 도 11B는 플레이 이후에 기간의 시간을 정하고 시간이 정해진 플레이 기간을 디스플레이하면서 애플리케이션을 플레이하도록, 각각 클라이언트 및 서버에 의해 서로 작용하여 실행되는 모범적인 시간이 정해진 플레이 및 미터 사용보고 루틴(675a) 및 (675b)으로 구성된 절차를 결합하여 도시하는 흐름도이다,. 루틴(675)에서, 클라이언트 및 서버는 단계(200)에서 기간(플레이 시간)을 정하면서 애플리케이션을 플레이하도록 시간이 정해진 애플리케이션-플레이 서브루틴을 호출한다.

서버(8)는 단계(210)로 진행되고, 여기서 클라이언트는 도 10B의 단계(92)에서와 같은 방법으로 TOU 코드에 따라 관련된 미터를 업데이트한다. 특히, TOU 코드가 0xH이면, 플레이 시간은 도표(60)에서 VIDv 및 NOv-i에 의해 식별되는 기록의 VM-LMETERv-i 필드값에 부가된다. TOU 코드가 axH(a : 볼륨에서 지정된 애플리케이션의 애플리케이션 번호)이면, 플레이 시간은 도표(60)에서 VIDv, NOv-i, 및 AIDv-i-a에 의해 식별되는 기록의 AM-METERv-i-a 필드값에 부가된다. 이어서, 서버(8)는 단계(212)에서 플레이 시간 및 업데이트된 미터값(즉, 총 플레이 시간량)을 네트워크 어드레스가 CADDc인 클라이언트에 전달하고, 처리 과정을 종료한다.

한편, 단계(200) 이후에 클라이언트(2)은 단계(214)에서 SIDs의 서버로부터 응답이 있는가를 보도록 시험한다. 이 단계는 클라이언트(2)이 서버(8)로부터 호출을 수신할 때까지 반복되고, 그 때 클라이언트(2)는 단계(216)에서 업데이트된 미터값이나 들어오는 메시지를 수신한다. 다음 단계(218)에서는 클라이언트(2)이 플레이 시간 및 총 플레이 시간량을 디스플레이하고, 이어서 루틴(675)을 종료한다.

도 12A 및 12B는 기간의 시간을 정하면서 애플리케이션을 플레이하도록, 각각 클라이언트(2) 및 서버(8)에 의해 실행되는 모범적인 시간이 정해진 애플리케이션-플레이 서브루틴(205a) 및 (205b)으로 구성된 절차를 결합하여 도시한 흐름도이다. SIDs의 서버(8)는 클라이언트의 애플리케이션 플레이를 시작하였는가를 보도록 단계(611)에서 통보를 대기한다. 한편, CADDc의 클라이언트(2)은 단계(610)에서 서버에게 플레이의 시작을 알리고, 단계(612)에서 바로 애플리케이션 플레이 서브 루틴을 호출한다. 이는 서버(8)가 단계(613)에서 타이머를 시작하도록 하고, 단계(615)에서 클라이언트(2)으로부터 플레이 중지 통보를 대기한다. 단계(612)를 완료하면, 클라이언트는 단계(614)에서 서버(8)에게 플레이 중단을 알린다. 이 통보에 응답해, 서버(8)는 단계(617)에서 타이머를 중지시키고 이를 플레이 시간으로 판독한다. 단계(614) 및 단계(617) 이후에 클라이언트 및 서버는 복귀된다.

비록 상술된 배열은 서버의 타이머를 사용하지만, 클라이언트의 타이머를 사용하는 것도 가능하다.

도 13A 및 도 13B는 각각 클라이언트(2) 및 서버(8)에 의해 서로 작용하여 실행되는 다른 방법의 시간이 정해진 애플리케이션-플레이 서브루틴(205ac) 및 (205bc)으로 구성된 절차를 결합하여 도시한 흐름도로, 플레이 시간의 타이밍이 클라이언트내의 타이머로 이루어진다. 다른 방법의 서브루틴(205a)에서, 클라이언트(2)은 단계(620)에서 타이머를 시작하고, 단계(622)에서 애플리케이션 플레이 루틴을 호출하고, 단계(624)에서 타이머를 중단시키고, 단계(626)에서 플레이 시간을 서버(8)에 전하고, 또한 복귀한다. 한편, 서브루틴(295b)으로 들어간 서버(8)는 단계(621)에서 CADDc의 클라이언트로부터 호출을 대기한다. 클라이언트(2)로부터 호출이 있으면, 서버(8)는 단계(623)에서 플레이 시간을 수신하고, 이어서 복귀한다.

그러나, 도 13의 배열은 불성실 사용자가 클라이언트(2)의 타이머를 조작하는 것을 허용할 가능성을 갖는다. 이점에서, 도 12에 도시된 배열이 도 13의 배열 보다 바람직하다.

도 14는 각각 도 12A 및 도 13A의 단계(612) 및 (622)에서 호출되고 제어기(100)에 의해 실행되는 모범적인 플레이 서브루틴의 흐름도이다.

흐름도의 설명에 앞서, 암호화 및 해독에 관한 일부 표시가 정의된다. 암호화 알고리즘 e에 따라 키(EK)로 X를 암호화하는 것이 Y를 산출하면, 이는 다음과 같이 표시된다:

e(EK, X) = Y

유사하게, 해독 알고리즘 d에 따라 키(DK)로 Y를 해독하는 것이 Z를 산출하면, 이는 다음과 같이 표시된다:

d(DK, Y) = Z

알고리즘 e 및 d와 키(EK) 및 (DK)가 서로 대응하는 것으로 가정하면, 즉 d(DK, Y) = X이면, 다음으로 이어진다:

d(DK, e(EK, X)) = X

다시 도 14를 참고로, 제어기(100)는 단계(602)에서 DVD의 분포 설명자(23)중 필드(32)로부터 PKu-암호화 애플리케이션-암호화 (AP-암호화) 키(Kv) 또는 e1(PKu, Kv)를 판독한다. 이때,

v = 1, 2, ..., V

여기서는 V는 애플리케이션 패키지의 종류의 수이다. 이는 다른 애플리케이션-암호화 키 K1 내지 Kv가 각 종류의 애플리케이션, 즉 볼륨 VID1 내지 VIDv에 지정됨을 나타낸다.

다음 단계(604)에서는 IC 카드(5)로부터 사용자 비밀키(SKu)가 판독된다. 다음 단계(606)에서, PKu-암호화 AP-암호화키 e1(PKu, Kv)는 애플리케이션 암호화 키(Kv)를 구하기 위해 사용자 비밀키(SKu)로 해독된다. 다음 단계(608)에서, Kv-암호화 애플리케이션(AP), 즉 DVD(3)에 기록된 e(Kv, AP)는 d(Kv, e(Kv, e(Kv, AP)) = AP를 구하기 위해 구해진 AP-암호화 키 Kv로 해독되고, 구해진 애플리케이션 데이터는 비디오 및 오디오 출력 IF(140)로 전달된다. 구해진 애플리케이션 데이터 MPEG 2 비트열의 형태를 갖는다. 비디오 및 오디오 출력 IF(140)는 애플리케이션 데이터의 MPEG 2 비트열을 MPEG 2 비디오 및 오디오 복호화를 통해 비디오 및 오디오 출력 신호를 변환시킨다. 비디오 및 오디오 출력 신호는 각각 디스플레이 장치(146) 및 스피커(148)로 인가된다.

사용 감지 청구 시스템으로 애플리케이션을 플레이

도 15는 도 5의 단계(700)로 도시된 유료 플레이 처리(700)의 절차를 도시하는 흐름도이고, 여기서 두 개의 흐름선으로 인접한 블록을 연결시키는 것은 각 블록이 CADDc의 클라이언트 및 SIDs의 연관된 서버에 의해 서로 작용하여 실행됨을 나타낸다. 도 15에서, 클라이언트(2)는 도 5의 단계(516)를 통해 처리(700)으로 들어가고, 여기서 클라이언트(2) 및 연관된 서버(8)는 초기화 루틴(80)을 실행한다. 다음 블록(640)에서, 클라이언트(2)는 서버(8)로부터 수신된 총 청구량과 예상 청구를 디스플레이하고, 사용자에게 원하는 애플리케이션을 플레이할 것인가 여부를 결정하도록 한다.

도 16A 및 도 16B는 각각 클라이언트(2) 및 연관된 서버(8)에 의해 서로 작용하여 실행되는 모범적인 기대 청구 통보 루틴(640a) 및 (640b)으로 구성된 절차를 결합하여 도시하는 흐름도이다. 루틴(640a) 및 (640b)는 루틴(640)에서 DURATION(Dn) 또는 플레이 시간이 RATE PER ACCESS 및 청구로 대치되고 ; 단계(92a)와 (93a) 사이에서 서버가 메모리 위치 R'에 의사 랜덤수(pseudo randomnumber) R을 발생하여 저장하는 단계(641)를 부가하고; 단계(93a)에서 서버가 의사 랜덤수 R를 또한 전달하고; 단계 (94)와 (95a) 사이에서 클라이언트가 순차적으로 사용되도록 메모리 위치 R에 수신된 의사 랜덤수 R를 저장하는 단계(643)를 부가하는 것을 제외하면, 루틴(97)과 매우 유사하다. DURATION(Dn)을 RATE PER ACCESS로 대치하는 것은 도표(70)에서 DURATION 필드(73) 대신에 RATE PER ACCESS 필드(74)를 억세스함으로써 이루어진다. 또한, 루틴(640)에서는 다음의 단계가 부가된다: 단계(96a)에 이어지는 단계(644)에서, 클라이언트(2)는 사용자가 애플리케이션을 플레이하기로 결정하는가를 보도록 점검이 이루어지고; 그렇지 않으면, 클라이언트(2)은 단계(645)에서 중지 메시지를 SADDs의 서버에 전달하고 루틴(640)을 종료한다; 한편, 단계(93a)에 이어지는 단계(642)에서, SIDs의 서버(8)는 CADDc의 클라이언트(2)로부터의 호출을 대기하고; 클라이언트로부터 호출을 수신하면, 서버는 수신된 것이 중지 메시지인가를 보도록 단계(646)에서 또 다른 점검을 실행하고; 그런 경우에 클라이언트는 루틴(640)을 종료한다; 또한, 사용자가 단계(644)에서 애플리케이션을 플레이하기로 결정하였으면, 즉 이후 설명으로부터 알 수 있는 바와 같이 서버가 수신한 것이 중지 메시지가 아니고 암호화 신용 카드 번호이면, 클라이언트(2) 및 서버(8)는 도 15의 단계(650)로 진행된다.

다음 블록(650)에서, 서버(8)는 도 17A 및 도 17B에 도시된 바와 같이 카드 번호의 신용을 유지하면서 클라이언트(2)를 통해 사용자의 신용 카드 번호(CCNOu)를 구한다. 단계(647)에서, 클라이언트(2)는 e2(R, CCNOu)를 구하도록 키, 즉 도 16A의 단계(643)에서 메모리 위치 R에 저장된 의사 랜덤수 R로 휴먼 IF(110)를 통해 사용자에 의해 입력된 사용자의 신용 카드 번호를 암호화한다. 다음 단계(648)에서, 클라이언트(2)는 또한 DVD의 버스트 절단 영역에 기록되는 분포 설명자(23)로부터 판독된 서버 공중키 또는 또 다른 키로 R + e2(R, CCNOu)를 암호화하여 다음을 구한다:

e1(PKs, R + e2(R, CCNOu))

다음 단계(649)에서, 클라이언트(2)는 암호화된 데이터를 서버(8)에 전달한다. 도 16B의 단계(646)을 통해, 서버는 단계(650)로 진행되고, 여기서 서버(8)는 클라이언트 CADDc로부터 수신된 것이 암호화된 데이터임을 발견한다. 다음 단계(651)에서, 서버(8)는 IC 카드(7)로부터 서버 비밀키(SKs) 를 판독하고, 다음 단계에서는 서버(8)가 수신된 암호화 데이터를 다음과 같이 서버 비밀키(SKs)로 해독한다:

d1(SKs, 암호화 데이터) = d1(SKs. e1(PKs, R + e2(R, CCNOu)) = R +e2(R, CCNOu)

단계(653)에서, 서버(8)는 막 구해진 의사 랜덤수 R가 서버의 메모리 위치 R'에 저장된 랜덤수 R와 일치하는가를 보도록 점검을 실행한다. 그런 경우, 서버(8)는 인에이블 메시지를 CAODc 의 클라이언트에 전달하고, 단계(655)에서 사용자의 신용 카드 번호(CCNOu)를 구하도록 의사 랜덤수 R로 e2(R, CCNOu)를 해독한다. 한편, 단계(657)에서의 인에이블 메시지의 수신에 응답해, 처리 과정으로부터 클라이언트(2)가 빠져나온다. 단계(655) 이후에는 또한 처리 과정으로부터 서버가 빠져나온다. 단계(653)에서 결과가 NO이면,서버(8)는 단계(656)에서 디스에이블 메시지를 클라이언트에 전달하고 처리를 종료한다. 단계(656)에서의 디스에이블 메시지의 수신에 응답해, 클라이언트는 단계(658)에서 이러한 취지로 메시지를 디스플레이하고, 처리를 종료한다.

블록(650)의 동작 이후에, 신용 카드가 유효한가를 보도록 단계(661)에서 서버(8)가 신용 카드와 연관된 신용 회사를 참고하는 동안, 클라이언트(2)는 단계(663)에서 전송된 카드 번호(CCNOu)에 대한 신용 카드가 유효한가 여부에 관한 서버로부터의 보고를 대기한다. 그렇지 않으면, 서버(8)는 단계(662)에서 클라이언트(2)에게 신용 카드의 무효를 통보하고 처리를 종료한다. 단계(661)에서 카드가 유효하면, 서버(8)는 단계(667)에서 클라이언트에게 유효함을 통보한다. 클라이언트(2)가 단계(663)에서 서버로부터 보고를 수신하면, 클라이언트는 보고가 카드의 유효함을 나타내는가를 보도록 단계(664)에서 또 다른 점검을 실행한다. 그렇지 않은 경우, 클라이언트는 단계(665)에서 무효를 나타내는 메시지를 디스플레이하고 처리를 종료한다. 보고가 단계(664)에서 단계(667)의 완료를 의미하는 유효함을 나타내면, 클라이언트(2) 및 서버(8)는 다음 블록(670)으로 전행된다.

단계(670)에서, 클라이언트(2) 및 서버(8)는 시간이 정해진 플레이 및 미터 청구 보고 루틴을 실행한다. 도 18A 및 도 18B는 기간의 시간을 정하고 플레이 이후에 요금 및 총 청구량을 디스플레이하면서 애플리케이션을 플레이하도록 서로 작용하여 실행되는 루틴(675ac) 및 (675bc)으로 구성된 절차를 결합하여 도시하는 흐름도이다. 도 18에서, 루틴(675ac) 및 (675bc)는 시간이 청구로 대치되고, 그에 따라 VM-METER가 VC-METER 및 AM-METER 및 AC-METER로 대치되는 것을 제외하면 도 11A 및 도 11B에서의 루틴(675a) 및 (675b)와 동일하다.

클라이언트 장치(2)에서 사용 감지 청구로 애플리케이션을 플레이하는 동작은 도 15의 블록(675) 또는 도 18A의 단계(218a)에 의해 완료된다. 단계(212a) 이후에, 서버(8)는 단계(680)에서 도 17B의 단계(655)에서 얻어진 신용 카드 번호(CCNOu)에 플레이에 대한 청구를 한다. 이는 도 15의 청구 애플리케이션 플레이 처리 과정 전체를 완료한다.

이러한 처리에서는 사용자에게 유료 정보만이 제공된다. 루틴(640b) 및 (640a)에 단계(91) 내지 (93) 및 (95)를 부가하고 루틴(675a) 및 (675ac)에 단계(210) 및 (218)을 부가함으로써 시간과 청구 모두에 대한 정보를 제공하는 것이 매우 쉽다.

상술된 바와 같이, 예상 기간 및/또는 청구는 사용자 지정 애플리케이션을 플레이하기 전에 디스플레이된다. 이는 사용자가 애플리케이션을 플레이할 것인가를 여부를 결정하는데 도움이 된다. 부가하여, 요금 청구는 실제적으로 시간이 정해진 플레이 기간을 근거로 행해진다. 이는 요금 청구를 합리적으로 만든다.

상기의 설명에서의 배열은 사용자가 애플리케이션을 플레이하기 원할 때마다 신용 카드 번호(CCNOu)를 입력하는 것이다. 그러나, 이 대신에 신용 카드 번호(CCNOu)는 PWu-암호화 형태로 비휘발성 메모리나 EEPROM(103)에 저장될 수 있다. 이러한 경우에, CCNOu는 사용자가 입력한 패스워드(password)로 PWu-암호화 CCNOu(예를 들면, e(PWu, CCNOu)를 복호화 함으로써 구해진다,. 즉, d(입력된 패스워드, e(PWu, CCNOu)) = CCNOu이다.

미리 지정된 한계내에서 플레이를 허용

도 19는 도 5의 동작 블록(800)에서 클라이언트(2) 및 서버(8)에 의해 서로 작용되어 실행되는 절차를 도시하는 흐름도이고, 여기서 두 개의 흐름선을 연결된 블록은 블록의 동작이 두 소자(2) 및 (8)에 의해 행해짐을 나타낸다. 이 경우에서는 미리 설정된 제한이 애플리케이션 패키지에 기록되고 매 플레이 시간에 클라이언트(2)로부터 서버(8)로 전달되는 것으로 가정된다. 도 5의 단계(516)를 통해 처리(800)를 들어가면, 클라이언트(2)는 단계(801)로 진행되고, 여기서 클라이언트(2) 및 서버(8)는 초기화 루틴(80)을 실행한다. 루틴(80b)에서, VIDv 및 NOv-i에 대한 기록이 있으면, 도 6A의 도표(60) 중 제한값(LVv-i) 필드는 클라이언트(2)로부터 전송된 제한값을 포함하고, 그렇지 않은 경우에는 단계(88)에서 VIDv 및 NOv-i에 대한 기록이 부가될 때 수신된 제한값이 LVv-i에 저장된다.

단계(810)에서, 서버(8)는, 클라이언트(2)으로부터 수신된 TOU 코드와 연관되는 미터가 제한값 이하에 있는가를 점검한다. 이러한 점검은 도표(60)에서 TOU 코드와 연관되는 LV 필드 및 LV-미터 필드를 비교함으로써 이루어진다. LV-미터값이 LV-필드값보다 크거나 같으면, 서버는 단계(820)에서 클라이언트(2)에 과도 제한 메시지를 복귀시킨다. 그렇지 않은 경우, 서버(8)는 단계(822)에서 클라이언트(2)에 과소 제한 메시지를 복귀시키고, 단계(828)로 진행된다. 클라이언트(2)가 단계(824)에서 과도 제한 메시지를 수신하면, 클라이언트(2)는 이점에 대해 메시지를 디스플레이한다. 그렇지 않은 경우, 클라이언트(2)는 단계(828)로 진행된다.

예상 플레이 시간 통보 루틴(97a) 및 (97b)와 애플리케이션 플레이 서브루틴(600)이 상술되었으므로, 단계(828) 및 (830)의 설명은 생략된다.

본 발명의 특성에 따라, 유료 정보의 사용을 제한하는 것이 가능하다. 이러한 특성은 특히 애플리케이션 패키지의 사용 항목으로 미리 지불한 사용자가 제한값내에서 애플리케이션 패키지를 사용하도록 허용된 경우에 유용하다.

비록 제한값이 애플리케이션 패키지에 포함되는 것으로 가정되었지만, 제한값은 처음부터 제공자나 분포자의 서버에 유지될 수 있다. 이러한 경우에는 제한값이 고정된다. 그러나, 제한값이 설정되어 분포 또는 판매시 애플리케이션 패키지에 기록되도록 허용되면, 제한값은 유리하게 지불된 양에 따라 설정된다.

상기로부터 명백한 바와 같이, 제한값으로서는 양으로 측정될 수 있는 사용제한 요소가 사용된다. 이러한 제한값을 예로 들면, 유효 날짜 및 시간, 허용가능한 만기 날짜 및 시간, 플레이 시간의 최대량, 허용가능한 억세스 카운트가 있다.

또한, 이러한 특성을 유효 애플리케이션 플레이 특성과 조합시키는 것이 가능하다. 즉, TOU와 연관된 LV-미터가 분포 설명자(23)의 필드(33) 또는 (34)에 기록된 값이나 대응하는 LV값 이하인 경우에만 사용자가 사용 감지 청구로 애플리케이션 패키지를 사용하도록 허용되는 배열이 있다.

[수정 I]

상기의 실시예에서, 애플리케이션, 하나 이상인 경우에는 한 볼륨내의 애플리케이션은 동일한 애플리케이션 암호화 키(Kv)에 의해 암호화된다. 그러나, 한 볼륨내의 애플리케이션(APa)은 각 AP-암호화 키 Ka로 암호화될 수 있다. 여기서, AP및 K에 이어지는 소문자 a는 각 애플리케이션 ID에 지정된 일련 번호이다. 이러한 경우에 각 AP-암호화 키 Ka는 사용자 공중키 PKu로 암호화되어, 분포 설명자(23)의 PKu-암호화 AP-암호화 키(Ka) 필드(32a)에 저장된다.

[수정 II]

DVD(3)의 사용자는 DVD(3)에 기록된 PKu-암호화 AP-암호화 키(Kv)를 갖는 구매자에 제한되는 것으로 가정되었다. 그러나, 시스템은 소정의 사람들, 예를 들면 구매자의 가족원 FM1, FM2, ...FMN(N은 가족원의 수)이 DVD를 사용할 수 있도록 배열될 수 있다. 이를 실현하는 방법 중 하나는 e1(PKu-1, Kv), e1(PKu-2, Kv), ..., e1(PKu-n, Kv)를 구하고 DVD의 구매시 분포 설명자(23)의 PKu-n-암호화 AP-암호화 키 e1(PKu-n, Kv) 필드(32)에 이를 기록하도록 각 멤버 FMn(n = 1, 2, ..., N)의 공중키(PKu-n)로 AP-암호화 키 Kv를 암호화하는 것이다.

[수정 III : 서버로부터의 Kv 회복]

상기의 설명에서, AP-암호화 키 Kv는 PKu-암호화 형태로 DVD(3)상에 기록되었다. 그러나, AP-암호화 키 Kv는 서버(8)에 의해 관리되고 DVD(3)를 사용할 때마다 DVD 플레이어(2)로부터 전해지는 요구에 응답해 클라이언트나 DVD 플레이어(2)로 전송될 수 있다. 이러한 경우에는 분포 설명자(23)에 PKu-암호화 AP-암호화 키 필드(32)를 제공할 필요가 없다. 대신에, 각 서버는 AP-암호화 키 도표 (또는 Kv 도표) 및 PKu 도표(도 20A 및 도 20B에 도시된)를 하드 디스크에 저장하여야 한다. 도 20A에 도시된 바와 같이, Kv 도표는 각 기록에서 볼륨 ID(VIDv) 필드(기록의 입력으로) 및 AP-암호화 키(Kv) 필드를 포함한다. 도 20B에서, PKu 도표의 각 기록은 볼륨 ID(VIDv) 필드(기록의 입력으로), 볼륨 발행 번호(NOv-i) 필드, 및 PKu 필드를 포함한다 (제 1 필드에서 연속하여 같은 값은 먼저 나타난 것만을 도시함으로써 도시된다). 또한, AP-암호화 키 Kv를 구하는 처리(또는 단계)(610), 즉 애플리케이션 플레이 루틴(600)에서 단계 (602), (604) 및 (606)의 그룹은 도 20C의 처리 과정으로 대치되어야 한다.

도 20C는 서버(8)로부터 클라이언트 DVD 플레이어(2)가 애플리케이션 암호화 키 Kv를 구하는 처리 과정의 흐름도이다. 단계(616)에서, 서버(8)는 VIDv를 이용하여 Kv 도표로부터 키 Kv를 회복시킨다. 다음 단계(618)에서는 키 Kv가 현재의 처리에서만 사용되는 임의의 수, 예를 들면 의사 랜덤수 R로 암호화되어 e2(R, Kv)를 구한다. 다음 단계(620)에서, 서버(8)는 각각 VIDv 및 NOv-i 필드에서 VIDv 및 NOv-i를 포함하는 기록의 PKu 필드를 판독함으로써 PKu 도표로부터 키 PKu를 회복시킨다. 다음 단계(622)에서, R + e2(R, Kv)는 다음의 이중 부호화 AP- 암호화 키를 구하도록 회복된 키 PKu로 암호화 되고,

e1(PKu, R + e2(R, Kv)

이는 다음 단계(624)에서 클라이언트 네트워크 어드레스 CADDc를 갖는 클라이언트로 복귀된다.

한편, 클라이언트(2)의 제어기(100)는 단계(626)에서 SIDs 서버(8)로부터 응답을 대기한다. 단계(626)에서 SIDs의 서버(8)로부터 응답이 있으며, 클라이언트 DVD(3)는 단계(628)에서 서버(8)로부터 데이터 e1(PKu, R + e2(R, Kv))를 수신한다. 다음 단계(630)에서, 수신된 데이터는 IC 카드(5)로부터 판독된 사용자 비밀키(SKu)로 해독된다. 특히, 다음의 계산이 행해진다.

d1(SKu, e1(PKu, R + e2(R, Kv))) => R + e2(R, Kv)

다음 단계(632)에서, e2(R, Kv)는 구해진 의사 랜덤수 R로 해독된다, 특히, 다음의 계산이 행해진다.

d2(R, e2(R, Kv) => Kv

이어서, 제어기(100)는 도 14의 단계(608)로 진행된다.

본 수정에서, 한 볼륨내에 애플리케이션(APa)은 각 AP-암호화 키 Ka로 암호화될 수 있다. 이러한 경우에, Kv 도표는 각 기록이 애플리케이션 ID(AIDa) 필드와 AP-암호화 키(Ka) 필드를 포함하는 Ka 도표로 대치되어야 한다. 또한, 단계(612)에서, DVD 플레이어(2)의 제어기(100)는 플레이될 애플리케이션의 애플리케이션 ID를 서버로 전달하여야 한다.

또한 본 수정에서, 시스템은 다시 소정의 사람들, 예를 들면 구매자의 가족원 FM1, FM2, ..., FMN(N은 가족원의 수)이 DVD를 사용할 수 있도록 배열될 수 있다. 이러한 경우에는 각 멤버 FMn(n = 1, 2, ..., N)에 대해 서버(8)가 AP-암호화 키 Kv를 암호화할 때 멤버의 자체 공중키 PKu-n을 사용하여야 한다. 이를 실현하는 한 방법은 DVD의 판매시 각 멤버(FMn)에 볼륨 발행 번호(NOv-i-n)를 전하고, 사용자의 패스워드(PWn)를 볼륨 발행 번호(NOv-i-n)와 연관시키도록 도표를 DVD 플레이어(2)의 비휘발성 메모리(도시되지 않은)에 제공하고, 단계(612)에서 사용자의 패스워드와 연관된 볼륨 발행 번호(NOv-i-n)를 전달하고, 또한 PKn 도표가 아닌 각 기록이 다음의 필드를 갖는 PKu-n 도표를 사용하는 것이다;

VIDv, NOv-i-n, PKu-n

또 다른 방법은 DVD의 판매시 모든 멤버에 대해 볼륨 발행 번호(NOv-i) 뿐만 아니라 가족원 번호(FMNn)을 발행 및 기록하고, 사용자의 패스워드(PWn)을 대응하는 가족원 번호(FMNn)와 연관시키도록 DVD 플레이어

(2)의 비휘발성 메모리(도시되지 않은)에 도표를 제공하고, 단계(612)에서 사용자의 패스워드와 연관된 가족원 번호(FMNn)와 볼륨 발행 번호(NOv-i)를 전하고, 또한 각 기록이 다음의 필드를 갖는 또 다른 PKu-n 테이블을 사용하는 것이다:

VIDv, NOv-i, FMNn, PKu-n

도 20C의 처리에서, 서버(8)는 서버 비밀키 및 공중키의 쌍(SKs, PKs)을 이용해 공중키 암호화시스템에 의해 인증된다. 이러한 경우, 서버(8)는 단계(622) 이후에 서버 비밀키(SKs)나 서명키로 다음의 이중-암호화 AP-암호화 키에 서명한다:

e1(PKu, R + e2(R, Kv)

클라이언트 또는 DVD 플레이어(2)는 단계(630) 이전에 DVD(2)의 버스트 절단 영역에 기록된 분포 설명자(23)의 PKs 필드(31)에 포함되는 서버 공중키 PKs나 시험 키로 서버(8)에 의한 서명을 시험한다.

그러나, 금방 설명된 서버(8)의 인증이 생략되더라도, 침입자는 TOU 코드 + 제한값, 볼륨 ID(VIDv), 볼륨 발행 번호(NOv-i), 및 클라이언트 네트워크 어드레스(CADDc)의 손실 보다 더 오래 가지는 않는다. 이는 심각한 문제가 아니다.

도 20C의 처리에서, 의사 랜덤수(R)는 처리 과정이 실행될 때마다 다른 값을 취하는 의사 변수로 사용되었다. 그러나, 암호화 결과가 처리 과정이 실행될 때마다 다른 값을 취하면, 의사 변수로 어느 것이든 될 수 있다.

[수정 IV]

제 1 실시예에서, 애플리케이션의 해독은 소프트웨어로 이루어진다. 이를 위해, 제어기(100)는 버스(102)를 통해 IC 카드(5)로부터 사용자 비밀키(SKu)를 판독해야 하여, 침입자가 버스(102)를 통해 사용자 비밀키(SKu)를 쉽게 훔치도록 허용할 가능성을 남긴다. 이를 방지하기 위해, 단계(604) 내지 (608)에 의해 이루어지는 처리 과정은 모범적인 내장 해독기 IC 카드 IF의 블록도인 도 21에 도시된 바와 같은 하드웨어로 이루어질 수 있다. 도 21에서, 내장 해독기 IC 카드 IF(120a)는 IC 카드 저장기(121)와 고정되고 그로부터 확장된 인쇄 배선 보드(122)를 포함한다. IC(123)는 인쇄 배선 보드(122)상에 설치된다. IC(123)는 통상 IC 카드(5)의 메모리를 버스(102)와 연결시키고, 제어기(100)로부터의 지시에 응답해 키(SKu)를 판독해 다음 스테이지에 전하는 메모리 IF(125); 키(SKu)를 수신하고 Kv를 산출하도록 e1(PKu, Kv)를 키(SKu)로 암호화하는 Kv 디코더(126); 및 키(Kv)를 수신하고 애플리케이션 데이터(AP)를 산출하도록 e(Kv, AP)를 암호화하는 AP 디코더(127)를 포함한다. 인쇄 배선 보드(122)부는 양호하게 전체적으로 단일 본체를 만들도록 IC 카드 저장기(121)부와 함께 몰드(mold) 처리된다. 이렇게 함으로써 사용자 비밀키(SKu)의 누설이 방지될 수 있다.

이러한 수정은 또한 도 20C의 암호화 시스템을 이용해 시스템 1에 적용될 수 있다. 이 경우에, 도 21의 Kv 디코더(126)는 도 22에 도시된 바와 같이 Kv 디코더(126a)와 대치되어야 한다. 도 22에서, Kv 디코더(126a)는 R + e2(R, Kv)를 구하도록 메모리 IF(125)에 의해 전해지는 사용자 비밀키(SKu)를 사용함으로써 버스(102)로부터의 입력 데이터, e1(PKu, R +e2(R, Kv)를 해독하고, 구해진 랜덤수(R)로 구해진 데이터 e2(R, Kv)를 해독하여 키(Kv)를 출력한다.

[실시예 II]

도 24는 본 발명의 제 2 실시예에 따라 서버와 통신하지 않고 DVD의 사용 항목으로 분포된 애플리케이션 패키지, 예를 들면 DVD를 플레이할 수 있는 시스템의 배열을 도시하는 블록도이다. 도 24에서, 시스템(1a)은 서버와의 통신이 필요 없기 때문에 통신 IF(150)가 제거되고, 제어기(100)가 제어기(100a)로 대치되는 것을 제외하면 도 1의 클라이언트 장치(21)와 동일하다. 제어기(100a)에서는 추후 기술된 바와 같이 제어 프로그램을 저장하기 위한 도시되지 않은 ROM과 EEPROM(103)이 또한 새로운 ROM(도시되지 않은)과 EEPROM(103a)으로 대치된다. 서버(8)의 역할을 플레이하기 위해, 시스템(1a)은 비휘발성 메모리, 예를 들면 EEPROM(103a)에 도 6A의 도표(60)를 포함하여야 하고, 도 6B의 도표(70)에서 정의된 바와 같은 각 애플리케이션에 대한 애플리케이션 기간(플레이 시간)은 각 애플리케이션 패키지의 제어 데이터에 포함되어야 한다.

도 25는 도 24에 도시된 제어기(100a)에 의해 실행되는 모범적인 제어 프로그램을 도시한다. 도 25의 제어 프로그램은 또한 본 실시예에서 제한 부착 플레이 모드가 시스템(1a)에 의해 지지되지 않기 때문에 결정 단계(516) 및 단계(700)가 제거되고, 단계(650) 및 (800)이 단계(650a) 및 (800a)로 대치되는 것을 제외하면 도 5와 동일하다. 따라서, 단계(514) 이후의 동작이 다음에서 설명된다.

결정 단계(514)에서 사용 항목(TOU) 코드의 하위 디지트가 001면, 단계(650a)에서 제어기(100a)는 단계(506) 또는 (512)에서 선택된 애플리케이션에 저장되는 애플리케이션을 무료 플레이 모드로 플레이하고, 동작을 종료한다. 시스템(1a)은 유료 플레이 모드를 포함하지 않으므로, TOU 코드의 하위 디지트는 다음과 같이 정의됨을 주목하여야 한다.

사용 형식		
비트에 설정	대응하는 제한값	운행 모드
더기트(10진수)		
0	없음	부분 운행 모드
2	유효 날짜 및 시간	제한 접속 운행 모드
3	허용가능한 만기 날짜 및 시간	
4	시청 주기의 최대값	
5	허용가능한 액세스 레벨	
	"	
	"	

따라서, 결정 단계(514)에서 TOU 코드의 하위 디지트가 00이 아니면, 단계(800a)에서 제어기(100a)는 단계(506) 또는 (512)에서 선택된 애플리케이션에 저장되는 애플리케이션을 제한 부착 플레이 모드로 플레이하고, 동작을 종료한다.

도 26 및 도 27은 각각 도 25의 단계(650a)에서 도시된 무료 플레이 모드의 동작을 상세한 형태 및 더 상세한 형태로 도시한다. 도 26에서, 제어기(100a)는 단계(660a)에서 초기화 루틴(80a)을 실행하고, 단계(670a)에서는 예상 플레이 시간 통보 루틴을 실행하고, 또한 단계(680a)에서는 애플리케이션 플레이 및 미터 플레이 시간 보고 루틴을 실행한다.

도 27에 도시된 바와 같이, 초기화 루틴(80c)에서, 제어기(100a)는 단계(86)에서 각각 볼륨 ID 및 발행 번호 필드에 VIDv 및 NOv-i를 포함하는 기록에 대해 도표(60)를 탐색한다. 탐색이 성공적이지 못하면, 제어기(100a)는 단계(88)에서 도표(60)에 있는 경우, VIDv 및 NOv-i에 대한 기록을 부가하고 AIDv-i-a 및 제한값으로 관련된 필드를 채운 후, 단계(90)로 진행된다. 또한, 단계(86)에서의 탐색이 성공적이면, 서버(9)는 단계(90)로 진행하고, 여기서 제어기(100a)는 TOU 코드값에 따라 다음에 실행될 루틴을 선택하고 선택된 루틴으로 들어간다. 이 경우에서, TOU 코드 = xOH (x : 임의의 HEX 수이고, 마지막 위치에 있는 문자 H는 진행되는 수가 16진수임을 나타낸다)이면, 무료로 애플리케이션을 플레이하는 루틴이 선택된다. TOU 코드 ≥ x1H이면, 사용자 제한 요소의 소프트웨어 미터가 미리 설정된 값 이하인 경우에만 애플리케이션을 플레이하는 루틴이 선택된다.

예상 플레이 시간 통보 루틴(670a)은 루틴(97)(도 10)-통신 단계(93) 및 (94)와 동일하며, 상술된 단계(91), (92), 및 (95)를 포함한다. 유사하게, 도 11 및 도 13A로부터 상술된 단계 (620), (622), (624), (210), 및 (218)는 시간 지정 플레이 및 미터 사용 보고 루틴(680a)에서 이 순서로 실행됨이 보여진다. 이러한 방법으로, 시스템(1a)은 사용자가 무료로 선택된 애플리케이션(도 25의 단계(506) 및 (512))에 저장된 애플리케이션을 플레이하도록 허용한다.

도 28은 도 25의 단계(800a)에서 도시된 제한 부착 플레이 모드의 동작을 도시하는 흐름도이다. 이 동작은 도 19와 매우 유사하므로, 흐름만이 간략하게 설명되고, 각 단계의 상세한 설명은 생략된다. 도 28에서, 제어기(100a)는 먼저 TOU 코드와 연관된 미터가 TOU 코드로 얻어진 제한값에 이르렀는가를 점검한다. 그런 경우, 서버는 단계(820)에서 제어기(100a)에 과도 제한 메시지를 복귀시킨다. 그렇지 않으면, 제어기(100a)는 예상 플레이 시간 통보 루틴(828a) (=670a)으로 진행되고, 여기서 제어기(100a)는 상술된 단계 (91), (92), 및 (95)를 실행하고, 단계(830)에서 애플리케이션 플레이 서브루틴(600)을 호출하고, 그에 의해 동작을 완료시킨다. 애플리케이션 플레이 서브루틴(600)은 상기에서 상세히 기술되었으므로, 더 이상의 설명은 생략된다. 이러한 방법으로, 시스템(1a)은 사용자 지정 애플리케이션 또는 볼륨에 지정된 TOC 코드와 연관되는 제한값에 이르지 않은 경우에만 사용자가 선택된 애플리케이션(도 25의 단계 (506) 및 (512))에 저장되는 애플리케이션을 플레이 하도록 허용한다.

제 2 실시예에 따라 시스템(1a)은 서버와의 통신이 필요 없이 무료 플레이 모드 및 제한 부착 플레이 모드 중 하나에서 동작될 수 있다. 그래서, 시스템(1a)은 휴대가능하게 만들어질 수 있다.

수정

상기의 설명에서, 설명된 실시예는 DVD와 연관되어 설명되었다. 같은 논의 내용이 한 번 이상의 기록을 허용하는 패키지 매체에도 적용될 수 있다.

또한, 본 발명은 또한 전송 매체를 통해 분포된 애플리케이션 패키지에도 적용가능하다. 이러한 경우에, 분포된 애플리케이션 패키지는 사용자 장치내의 벌크(bulk) 저장기에 저장된다. 애플리케이션 패키지는 하나 이상의 애플리케이션 및 애플리케이션 제어 데이터, 즉 애플리케이션 설명자 및 분포 설명자를 포함한다. 한 볼륨은 한 파일로 저장된다. 다수의 애플리케이션 패키지가 단일 저장기에 저장되므로, 각 애플리케이션 패키지는 제어 프로그램을 포함할 필요가 없다. 하나의 사용자 장치에는 패키지나 전송 매체를 통해 분포될 수 있는 하나의 제어 프로그램이면 충분하다. 애플리케이션 패키지가 저장된 폴더(folder)나 디렉토리(directory)는 제어 프로그램이 설치될 때 제어 프로그램에서 사용자가 지정한 것에 대해 설정된다. 분포 설명자에 저장되는 데이터는 사용자에 의해 주어진 정보에 따라 제공자에 의해 애플리케이션 패키지에 포함된다.

상술된 바와 같이, 애플리케이션 패키지를 사용하도록 허용되는 자는 애플리케이션 패키지에서 AP- 암호화 키 Kv의 암호화에 사용된 사용자 공중키(PKu)에 대응하는 사용자 비밀키(SKu)를 저장하는 IC 카드의 소유자로 제한된다. 그래서, 누군가가 예를 들면 볼륨이 기록된 DVD로부터 전체 볼륨을 복사함으로써 부당하게 구해진 애플리케이션 패키지를 갖더라도, DVD 소유자의 IC 카드가 없으면 이를 사용할 수 없다. 이와 같이, 본 발명의 시스템은 애플리케이션 패키지의 정규 소유자 이외의 다른 사람에 의한 애플리케이션 패키지(이 경우에는 DVD)의 부당한 사용을 방지할 수 있다.

또한, 본 발명의 시스템은 적어도 볼륨 제어 데이터(즉, 분포 설명자)의 일부가 제작 처리 이후에 예를

들면, 각 DVD의 분포시 결정될 수 있는 반면, 애플리케이션 패키지의 대부분의 DVD의 제작 처리에서 압박을 가함으로써 기록되도록 배열된다. 이는 제어 데이터가 날인을 변화시키지 않고 용이하게 변화될 수 있기 때문에 시스템을 탄력성 있게 만든다.

도 8A 및 도 8B의 초기화 루틴(80a) 및 (80b)에서, 서비스 요구와 전송된 데이터는 도 17에 도시된 사용자의 신용 카드 번호를 전송하는 경우와 같은 방법으로 암호화된다. 그러나, 초기화 루틴의 경우에는 다수의 데이터가 있다. 이러한 데이터는 다음의 방법으로 암호화될 수 있다/

암호화되는 데이터가 D1, D2, ...이면, 이들은 먼저 다음과 같이 키(R)로 암호화된다:

e2(R, D1), e2(R, D2), ...

또 다른 암호화는 다음과 같이 서버 공중키(PKs)로 이루어진다:

e1(PKs, R + e2(R, D1), e2(R, DS), ...

그 동안 서버는 단계(650) 이전에 사용자 공중키(PKu)나 시험키로 클라이언트(2)에 의한 서명을 시험한다.

단일 서버 공중키를 분포 설명자(23)에 저장하는 대신에, 다수의 서버 공중키나 모든 서버 공중키가 기록된다. 이로 인해, 예를 들면, 사용자가 도표(70) 및 (75)를 적절히 조합하여 선택한 서버 공중키에 따라 다른 요금 청구를 설정하는 것이 가능하다.

또한, 동일한 볼륨 ID를 갖는 애플리케이션 패키지가 기록된 다른 서버 공중키를 갖을 수 있다. 다수의 톨 센터에는 유리하게 같은 제목의 애플리케이션 패키지가 제공될 수 있다.

IC 카드 소유자 이외의 사람이 IC 카드를 사용하는 것을 방지하기 위해서는 SKu 기록 단계(604) 이전에 사용자에게 휴먼 IF(110)를 통해 패스워드를 입력하도록 촉구하는 단계와, 입력된 패스워드가 IC 카드에 저장된 사용자 패스워드 PWu와 일치하는 경우에만 단계(604)로 진행되는 단계를 부가하는 것이 가능하다.

상기 실시예에서는 IC 카드(5)가 사용되지만, IC 카드 IF(120)는 자기 카드의 사용을 허용하도록 자기 카드 판독기와 대치될 수 있다. 다른 방법으로, 사용자가 DVD를 사용할 때마가 패스워드를 입력하도록 하는 배열이 있다.

IC 카드(5)에 사용자 비밀키(SKu)를 저장하는 대신에, 키(SKu)는 PWu-암호화 형태로 비휘발성 메모리에 저장될 수 있다. 이러한 경우에, 키(SKu)는 사용자가 입력한 패스워드로 PWu-암호화 SKu를 해독함으로서 구해진다.

3개의 선행하는 문단에서의 논의는 서버에 서버 비밀키를 저장하는데 사용되는 IC 카드에 적용된다. 그러나, 이러한 경우, 사용자는 톨 서버(toll server)로 취해져야 한다.

본 발명의 의도 및 범위에서 벗어나지 않고 폭넓게 다른 다수의 본 발명의 실시예가 구성될 수 있다. 본 발명은 첨부되는 청구항에서 정의된 바를 제외하고, 명세서에서 설명된 특정 실시예에 제한되지 않는 것으로 이해되어야 한다.

발명의 효과

내용 없음

(57) 청구의 범위

청구항 1

애플리케이션 패키지(package) (볼륨(volume))에 포함된 애플리케이션을 플레이하기 위한 시스템에 사용하기 위한 애플리케이션 패키지에 있어서,

적어도 하나의 애플리케이션을 위한 애플리케이션 데이터, 및

상기 시스템을 제어하는데 사용되는 볼륨 제어 데이터를 구비하고,

상기 볼륨 제어 데이터가 적어도

상기 애플리케이션 패키지(상기 볼륨)의 종류를 식별하는 볼륨 ID와,

상기 종류의 각 볼륨에 대한 발행 순서로 지정되는 발행 번호와,

상기 볼륨에 포함된 상기 적어도 하나의 애플리케이션 중 하나의 각각 지정된 애플리케이션 ID를 구비하고,

상기 볼륨 제어 데이터 중 적어도 일부가 상기 볼륨의 생성 이후에 상기 볼륨에 부가되고, 또한

상기 볼륨 제어 데이터 중 상기 적어도 일부가 상기 발행 번호를 포함하는 것을 특징으로 하는 애플리케이션 패키지.

청구항 2

제 1 항에 있어서,

상기 애플리케이션 데이터가 암호키로 암호화되고,

상기 볼륨 제어 데이터 중 상기 적어도 일부는 사용된 상기 암호키의 사용자 공중키(public key)-암호화 버전을 포함하는 것을 특징으로 하는 애플리케이션 패키지.

청구항 3

제 1 항에 있어서,

상기 볼륨 제어 데이터 중 상기 적어도 일부는 상기 볼륨 또는 상기 적어도 하나의 애플리케이션에 지장되는 모드 코드를 포함하고, 각각 모드 코드가 지정된 상기 볼륨 또는 상기 적어도 하나의 애플리케이션 중 하나와 관련된 플레이 모드를 나타내는 것을 특징으로 하는 애플리케이션 패키지.

청구항 4

제 1 항에서 정의된 바와 같은 애플리케이션 패키지가 기록되는 것을 특징으로 하는 패키지 매체.

청구항 5

제 1 항에서 정의된 바와 같이 애플리케이션 패키지가 기록되는 것을 특징으로 하는 1회 기록형의 패키지 매체.

청구항 6

제 1 항에서 정의된 바와 같은 애플리케이션 패키지가 기록되고, 상기 볼륨 제어 데이터 중 상기 적어도 일부는 상기 애플리케이션 데이터가 패키지 매체상에 기록된 데이터 영역과 다른 영역에 기록되는 것을 특징으로 하는 패키지 매체.

청구항 7

상승된 보안성을 갖는 데이터를 제 1 장치에서 공중 통신 네트워크를 통해 제 2 장치로 전달하는 방법에 있어서,

상기 제 2 장치에서,

의사 랜덤수를 발생하는 단계와,

상기 의사 랜덤수를 상기 제 1 장치에 전송하는 단계와,

상기 제 1 장치에서,

상기 전송된 의사 랜덤수를 사용해 상기 데이터를 암호화 데이터로 암호화하는 단계와,

상기 의사 랜덤수와 상기 암호화된 데이터로 구성된 연관 데이터를 상기 제 2 장치의 공중키를 이용해 이중-암호화 데이터로 암호화하는 단계와,

상기 이중-암호화 데이터를 상기 제 2 장치로 전달하는 단계와,

상기 제 2 장치에서,

상기 공중키에 대응하는 상기 제 2 장치의 비밀키를 사용해 상기 이중-암호화 데이터를 해독된 랜덤수 부분과 또 다른 해독 부분으로 구성되는 해독 데이터로 해독하는 단계와,

상기 데이터를 얻기 위하여 상기 전송된 랜덤수로 상기 또 다른 해독 부분을 해독하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 8

상승된 보안성을 갖는 다수의 데이터부를 제 1 장치에서 공중 통신 네트워크를 통해 제 2 장치로 전달하는 방법에 있어서,

상기 제 2 장치에서,

의사 랜덤수를 발생하는 단계와,

상기 의사 랜덤수를 상기 제 1 장치에 전송하는 단계와,

상기 제 1 장치에서,

상기 전송된 의사 랜덤수를 사용해 상기 각각의 데이터를 암호화 데이터부로 암호화하는 단계와,

상기 의사 랜덤수와 상기 암호화된 데이터부로 구성된 연관 데이터를 상기 제 2 장치의 공중키를 이용해 이중-암호화 데이터로 암호화하는 단계와,

상기 이중-암호화 데이터를 상기 제 2 장치로 전달하는 단계와,

상기 제 2 장치에서,

상기 공중키에 대응하는 상기 제 2 장치의 비밀키를 사용해 상기 이중-암호화 데이터를 해독된 랜덤수 부분과 다수의 해독 부분으로 구성되는 해독 데이터로 해독하는 단계와,

상기 데이터부를 얻기 위하여 상기 전송된 랜덤수로 상기 각 해독 부분을 해독하는 단계를 구비하는 것을 특징으로 하는 방법.

청구항 9

제 7 항 또는 제 8 항 중 한 항에 있어서,

상기 이중-암호화 데이터를 복호화하는 단계 이후에 실행되는,

상기 해독 랜덤수 부분이 상기 전송된 의사 랜덤수와 일치하는 경우에만 다음 단계로 진행되는 단계와,

상기 해독 랜덤수 부분이 상기 전송된 의사 랜덤수와 일치하지 않으면 상기 제 2 장치가 상기 제 1 장치에 해독 실패를 알리는 단계를 더 구비하는 것을 특징으로 하는 방법.

청구항 10

애플리케이션 패키지에 포함된 애플리케이션을 플레이하기 위한 수단이 제공되는 시스템에서, 사용자가 사용자의 비밀키를 이용해 암호키로 해독될 수 있도록 암호화된 사용자 공중키-암호화 암호키를 볼륨 제어 데이터로 더 포함하는 분포 애플리케이션 패키지내에 포함되는 암호키-암호화 애플리케이션을 플레이하는 것을 허용하는 방법에 있어서,

상기 분포된 애플리케이션 패키지(상기 볼륨)로부터 상기 사용자 공중키-암호화 암호키를 판독하는 단계와,

상기 비밀키를 구하는 단계와,

상기 암호키를 구하도록 상기 비밀키로 상기 사용자 공중키-암호화 암호키를 해독하는 단계와.

구해진 상기 암호키를 이용해 상기 암호키-암호화 애플리케이션을 애플리케이션 데이터로 해독하고, 동시에 애플리케이션을 플레이하기 위한 상기 수단에 상기 애플리케이션 데이터를 전달하는 단계를 구비하는 것을 특징으로 하는 방법.

청구항 11

애플리케이션 패키지에 포함된 애플리케이션을 플레이하기 위한 수단이 제공된 클라이언트 및 통신 네트워크를 통해 클라이언트와 연결된 서버(server)를 구비하는 시스템에서, 사용자가 분포된 애플리케이션 패키지(상기 볼륨)의 종류를 식별하기 위한 볼륨 ID, 발행된 순서로 각 종류의 볼륨에 부여되는 발행 번호, 및 애플리케이션 ID를 볼륨 제어 데이터로 더 포함하는 분포 애플리케이션 패키지내에 포함되는 암호키-암호화 애플리케이션 중 하나를 플레이하는 것을 허용하는 방법에 있어서,

상기 클라이언트가 상기 볼륨으로 부터 암호키-암호화 애플리케이션 중 상기 하나(상기 암호키-암호화 애플리케이션)에 대해 상기 볼륨 ID, 상기 발행 번호, 및 애플리케이션 ID를 판독하여 상기 서버에 전달하는 단계와.

상기 서버에서,

상기 볼륨 ID를 이용해 상기 암호키를 회복하는 단계와,

상기 볼륨 ID 및 상기 발행 번호를 이용해 상기 사용자의 공중키를 회복하는 단계와.

의사 랜덤수를 발생하는 단계와,

상기 의사 랜덤수 및 상기 공중키를 사용해 상기 암호키를 이중 암호화 데이터로 이중 -암호화하는 단계와.

상기 이중-암호화된 데이터를 상기 클라이언트에 전달하는 단계와,

상기 클라이언트에서,

상기 공중키에 대응하는 상기 사용자의 비밀키를 구하는 단계와.

상기 비밀키로 상기 이중-암호화된 데이터를 해독함으로서 상기 암호키를 구하는 단계와,

구해진 상기 암호키를 이용해 상기 암호키-암호화 애플리케이션을 애플리케이션 데이터로 해독하고, 동시에 애플리케이션을 플레이하기 위한 상기 수단에 상기 애플리케이션 데이터를 전달하는 단계를 구비하는 것을 특징으로 하는 방법.

청구항 12

제 10 항 또는 제 11 항 중 한 항에 있어서.

비밀키를 구하기 위한 상기 수단이 상기 사용자의 휴대용 메모리로부터 상기 비밀키를 판독하기 위한 수단을 구비하는 것을 특징으로 하는 방법.

청구항 13

제 12 항에 있어서,

상기 휴대용 메모리가 IC 카드인 것을 특징으로 하는 방법.

청구항 14

볼륨 ID 및 발행된 순서로 상기 볼륨 ID의 각 볼륨에 부여된 발행 번호를 볼륨 제어 데이터로 포함하는 애플리케이션 패키지(볼륨)를 플레이하기 위한 수단이 제공된 클라이언트 및 클라이언트를 제어하도록 통신 네트워크를 통해 클라이언트와 연결된 서버를 구비하는 시스템에서, 플레이 시간량을 제어하는 방법에 있어서,

상기 클라이언트가 상기 볼륨 ID 및 상기 발행 번호를 상기 서버에 전달하는 단계와.

상기 서버가 상기 볼륨 ID 및 상기 발행 번호와 연관된 예상 플레이 시간을 회복하는 단계와.

상기 서버가 상기 볼륨 ID 및 상기 발행 번호와 연관된 총 플레이 시간값에 상기 예상 플레이 시간을 부

가하는 단계를 구비하는 것을 특징으로 하는 방법.

청구항 15

볼륨 ID, 발행된 순서로 상기 볼륨 ID의 각 볼륨에 부여된 발행 번호, 및 애플리케이션에 대한 애플리케이션 ID를 볼륨 제어 데이터로 포함하는 애플리케이션 패키지(볼륨)에 포함된 애플리케이션을 플레이하기 위한 수단이 제공된 클라이언트 및 클라이언트를 제어하도록 통신 네트워크를 통해 클라이언트와 연결된 서버를 구비하는 시스템에서, 플레이 시간량을 제어하는 방법에 있어서,

상기 클라이언트가 상기 볼륨 ID, 상기 발행 번호, 및 상기 애플리케이션 ID를 상기 서버에 전달하는 단계와,

상기 서버가 상기 볼륨 ID 및 상기 발행 번호, 및 상기 애플리케이션 ID와 연관된 예상 플레이 시간을 회복하는 단계와,

상기 서버가 상기 볼륨 ID 및 상기 발행 번호와 연관된 총 플레이 시간값에 상기 기대 플레이 시간을 부가하는 단계를 구비하는 것을 특징으로 하는 방법.

청구항 16

볼륨 ID 및 발행된 순서로 상기 볼륨 ID의 각 볼륨에 부여된 발행 번호를 볼륨 제어 데이터로 포함하는 애플리케이션 패키지(볼륨)에 포함된 애플리케이션을 플레이하기 위한 수단이 제공된 클라이언트 및 클라이언트를 제어하도록 통신 네트워크를 통해 클라이언트와 연결된 서버를 구비하는 시스템에서, 플레이 시간량을 제어하는 방법에 있어서,

상기 클라이언트가 상기 서버가 상기 애플리케이션의 플레이 시간을 측정된 플레이 시간으로 서로 작용하여 측정하는 단계와,

상기 서버가 상기 볼륨 ID 및 상기 발행 번호와 연관된 총 플레이 시간값에 상기 측정된 플레이 시간을 부가하는 단계를 구비하는 것을 특징으로 하는 방법.

청구항 17

제 16 항에 있어서,

플레이 시간을 측정하는 상기 단계가 상기 서버의 타이머를 사용하는 단계를 구비하는 것을 특징으로 하는 방법.

청구항 18

제 16 항에 있어서,

플레이 시간을 측정하는 상기 단계가 상기 클라이언트의 타이머를 사용하는 단계를 구비하는 것을 특징으로 하는 방법.

청구항 19

애플리케이션 패키지를 플레이하는 클라이언트 및 통신 네트워크를 통해 클라이언트와 연결된 서버를 구비하고, 애플리케이션 패키지(볼륨)가 애플리케이션 데이터 및 제어 데이터를 포함하고, 또한 상기 볼륨의 생성 이후에 제어 데이터 중 적어도 일부가 볼륨에 부가되는 시스템에서, 원하는 데이터를 상기 클라이언트 및 상기 서버 중 한 측면에서 다른 측면으로 전달하는 방법에 있어서,

상기 제어 데이터 중 상기 적어도 일부에 상기 다른 측면의 비밀키를 포함하는 단계와,

상기 다른 측면에서,

의사 랜덤수를 발생하는 단계와,

상기 의사 랜덤수를 상기 한 측면에 전송하는 단계와,

상기 한 측면에서,

상기 전송된 의사 랜덤수를 사용해 상기 원하는 데이터를 암호화 데이터로 암호화 하는 단계와,

상기 다른 측면의 상기 공중키를 사용해 상기 의사 랜덤수와 상기 암호화 데이터로 구성된 연관 데이터를 이중-암호화 데이터로 암호화하는 단계와,

상기 이중-암호화 데이터를 상기 다른 측면에 전달하는 단계와,

상기 다른 측면에서,

상기 공중키에 대응하는 상기 다른 측면의 비밀키를 사용해 상기 이중-암호화 데이터를 해독된 랜덤수 부분과 또 다른 해독 부분으로 구성되는 해독 데이터로 해독하는 단계와,

상기 원하는 데이터를 구하도록 상기 전송된 랜덤수로 상기 또 다른 해독 부분을 해독하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 20

제 19 항에 있어서,

의사 랜덤수를 발생하는 상기 단계가 상기 의사 랜덤수를 메모리에 저장하는 것을 포함하고, 여기서 상기 또 다른 해독 부분을 해독하는 상기 단계 이전에 실행되는,

상기 해독된 랜덤수 부분이 상기 메모리에 저장된 상기 의사 랜덤수를 저장하기 위한 상기 수단에 저장되는 상기 의사 랜덤수와 일치하지 않는다는 결정에 응답해, 다음 수단에 제어를 전하는 대신에 상기 한 측면에 해독 실패를 알리는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 21

애플리케이션 패키지에 포함된 애플리케이션을 플레이하기 위한 수단이 제공된 클라이언트 및 통신 네트워크를 통해 클라이언트와 연결된 서버를 구비하는 시스템에서, 사용자가 분포된 애플리케이션 패키지(상기 볼륨)의 종류를 식별하기 위한 볼륨 ID, 발행된 순서로 각 종류의 볼륨에 부여되는 발행 번호, 및 상기 애플리케이션에 대한 애플리케이션 ID를 볼륨 제어 데이터로 더 포함하는 분포 애플리케이션 패키지내에 포함되는 애플리케이션을 플레이하는 것을 허용하는 방법에 있어서,

볼륨 데이터 도표에서 상기 볼륨 ID, 상기 발행 번호, 및 상기 애플리케이션 ID와 연관된 미터 필드(meter field)의 값이 상기 볼륨 ID, 상기 발행 번호, 및 상기 애플리케이션 ID와 연관된 제한값 필드의 값 이하인 경우에만 다음 단계로 진행되는 단계와,

디스플레이 장치에서 과도 제한을 상기 클라이언트에 알리는 메시지를 디스플레이하고, 그렇지 않은 경우 동작을 중단시키는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 22

애플리케이션 패키지에 포함된 애플리케이션을 플레이하기 위한 수단이 제공된 클라이언트 및 통신 네트워크를 통해 클라이언트와 연결된 서버를 구비하는 시스템에서, 사용자가 분포된 애플리케이션 패키지(상기 볼륨)의 종류를 식별하기 위한 볼륨 ID, 발행된 순서로 각 종류의 볼륨에 부여되는 발행 번호, 상기 애플리케이션에 대한 애플리케이션 ID, 및 상기 애플리케이션의 플레이를 제한하는 제한값을 볼륨 제어 데이터로 더 포함하는 분포 애플리케이션 패키지내에 포함되는 애플리케이션을 플레이하는 것을 허용하는 방법에 있어서,

볼륨 데이터 도표에서 상기 볼륨 ID, 상기 발행 번호, 및 상기 애플리케이션 ID와 연관된 미터 필드(meter field)의 값이 상기 제한값 이하인 경우에만 다음 단계로 진행되는 단계와,

디스플레이 장치에서 과도 제한을 상기 클라이언트에 알리는 메시지를 디스플레이하고, 그렇지 않은 경우 동작을 중단시키는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 23

제 21 항에 있어서,

상기 제한값이 유효 날짜 및 시간, 허용가능한 만기 날짜 및 시간, 플레이 시간의 최대량, 또한 허용가능한 억세스 카운트 중 하나인 것을 특징으로 하는 방법.

청구항 24

제 11 항, 제 15 항, 및 제 16 항 중 어느 한 항에 있어서,

상기 클라이언트가 상기 서버에 전달하는 상기 단계가

상기 클라이언트가 상기 볼륨 ID, 상기 발행 번호, 및 상기 애플리케이션 ID 중 적어도 하나를 암호화 데이터로 암호화하는 단계와,

상기 서버가 상기 암호화 데이터를 해독하는 단계를 구비하는 것을 특징으로 하는 방법.

청구항 25

상승된 보안성을 갖는 데이터를 제 1 장치에서 공중 통신 네트워크를 통해 제 2 장치로 전달하는 시스템에 있어서,

의사 랜덤수를 발생하기 위해 상기 제 2 장치에 제공되는 수단과,

상기 의사 랜덤수를 상기 제 1 장치에 전송하기 위해 상기 제 2 장치에 제공되는 수단과,

상기 전송된 의사 랜덤수를 사용해 상기 데이터를 암호화 데이터로 암호화하기 위해 상기 제 1 장치에 제공되는 수단과,

상기 의사 랜덤수와 상기 암호화된 데이터로 구성된 연관 데이터를 상기 제 2 장치의 공중키를 이용해 이중-암호화 데이터로 암호화하기 위해 상기 제 1 장치에 제공되는 수단과,

상기 이중-암호화 데이터를 상기 제 2 장치로 전달하기 위해 상기 제 1 장치에 제공되는 수단과,

상기 공중키에 대응하는 상기 제 2 장치의 비밀키를 사용해 상기 이중-암호화 데이터를 해독된 랜덤수 부분과 또 다른 해독 부분으로 구성되는 해독 데이터로 해독하기 위해 상기 제 2 장치에 제공되는 수단과,

상기 데이터를 구하도록 상기 전송된 랜덤수로 상기 또 다른 해독 부분을 해독하기 위해 상기 제 2 장치에 제공되는 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 26

상승된 보안성을 갖는 다수의 데이터 일부를 제 1 장치에서 공중 통신 네트워크를 통해 제 2 장치로 전달하는 시스템에 있어서,

의사 랜덤수를 발생하기 위해 상기 제 2 장치에 제공되는 수단과,

상기 의사 랜덤수를 상기 제 1 장치에 전송하기 위해 상기 제 2 장치에 제공되는 수단과,

상기 전송된 의사 랜덤수를 사용해 상기 각 데이터 일부를 암호화 데이터 일부로 암호화하기 위해 상기 제 1 장치에 제공되는 수단과,

상기 의사 랜덤수와 상기 암호화된 데이터 일부로 구성된 연관 데이터를 상기 제 2 장치의 공증키를 이용해 이중-암호화 데이터로 암호화하기 위해 상기 제 1 장치에 제공되는 수단과,

상기 이중-암호화 데이터를 상기 제 2 장치로 전달하기 위해 상기 제 1 장치에 제공되는 수단과,

상기 공증키에 대응하는 상기 제 2 장치의 비밀키를 사용해 상기 이중-암호화 데이터를 해독 된 랜덤수 부분과 상기 다수의 해독 부분으로 구성되는 해독 데이터로 해독하기 위해 상기 제 2 장치에 제공되는 수단과,

상기 데이터 일부를 구하도록 상기 전송된 랜덤수로 상기 각 해독 부분을 해독하기 위해 상기 제 2 장치에 제공되는 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 27

제 25 항 또는 제 26 항 중 한 항에 있어서,

상기 제 2 장치에 제공되고, 상기 각 해독 부분을 해독하기 전에 활성화되고, 상기 해독된 랜덤수 부분이 상기 전송된 의사 랜덤수와 일치하지 않는다는 결정에 응답해, 다음 수단에 제어를 전하는 대신에 상기 제 1 장치에 해독 실패를 알리는 수단을 더 구비하는 것을 특징으로 하는 시스템.

청구항 28

사용자의 비밀키를 이용해 암호키로 해독될 수 있도록 암호화된 사용자 공증키-암호화 암호키를 볼륨 제어 데이터로 더 포함하는 분포 애플리케이션 패키지 내에 포함되는 암호키-암호화 애플리케이션을 플레이하는 시스템에 있어서,

상기 분포 애플리케이션 패키지(상기 볼륨)로부터 상기 사용자 공증키-암호화 암호키를 판독하는 수단과,

상기 비밀키를 구하는 수단과,

상기 암호키를 구하도록 상기 비밀키로 상기 사용자 공증키-암호화 암호키를 해독하는 수단과,

애플리케이션 데이터를 제공하도록 상기 구해진 암호키로 상기 암호키-암호화 애플리케이션을 해독하는 수단과,

플레이를 위해 상기 애플리케이션 데이터를 사용하는 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 29

사용자가 분포된 애플리케이션 패키지(상기 볼륨)의 종류를 식별하기 위한 볼륨 ID, 발행된 순서로 각 종류의 볼륨에 부여되는 발행 번호, 및 애플리케이션 ID를 볼륨 제어 데이터로 더 포함하는 분포 애플리케이션 패키지내에 포함되는 암호키-암호화 애플리케이션 중 하나를 플레이하는 것을 허용하는 시스템에 있어서,

애플리케이션 데이터를 이용함으로써 애플리케이션을 플레이하는 클라이언트와,

통신 네트워크를 통해 상기클라이언트를 제어하는 서버를 구비하고,

상기 클라이언트가

상기 볼륨으로부터 암호키-암호화 애플리케이션 중 상기 하나(상기 암호키-암호화 애플리케이션)에 대해 상기 볼륨 ID, 상기 발행번호, 및 애플리케이션 ID를 판독하여 상기 서버에 전달하는 수단을 구비하고,

상기 서버가

상기 볼륨 ID를 이용해 상기 암호키를 회복하는 수단과,

상기 볼륨 ID 및 상기 발행번호를 이용해 상기 사용자의 공증키를 회복하는 수단과,

의사 랜덤수를 발생하는 수단과,

상기 의사 랜덤수 및 상기 공증키를 사용해 상기 암호키를 이중 암호화 데이터로 이중-암호화하는 수단과,

상기 이중-암호화된 데이터를 상기 클라이언트에 전달하는 수단을 구비하고,

상기 클라이언트가

상기 공증키에 대응하는 상기 사용자의 비밀키를 구하는 수단과,

상기 비밀키로 상기 이중-암호화된 데이터를 해독함으로서 상기 암호키를 구하는 수단과,

애플리케이션 데이터를 제공하도록 구해진 상기 암호키로 상기 암호키-암호화 애플리케이션을 해독하는 수단과,

플레이하기 위해 상기 애플리케이션 데이터를 이용하는 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 30

제 28 항 또는 제 29 항에 있어서,

비밀키를 구하는 상기 수단이 상기 사용자의 휴대용 메모리로부터 상기 비밀키를 판독하기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 31

제 30 항에 있어서,

상기 휴대용 메모리가 IC 카드인 것을 특징으로 하는 시스템.

청구항 32

사용자가 볼륨 제어 데이터로서 분포된 애플리케이션 패키지(상기 볼륨)의 종류를 식별하기 위한 볼륨 ID 및 발행된 순서로 각 종류의 볼륨에 부여되는 발행 번호를 더 포함하는 분포 애플리케이션 패키지를 플레이하는 것을 허용하는 시스템에 있어서,

상기 분포된 애플리케이션 패키지를 플레이하는 클라이언트와,

통신 네트워크를 통해 상기 클라이언트를 제어하는 서버를 구비하고,

상기 클라이언트가 상기 볼륨 ID 및 상기 발행 번호를 상기 서버에 전달하기 위한 수단을 구비하고, 또한,

상기 서버가 상기 볼륨 ID 및 상기 발행 번호와 연관된 예상 플레이 시간을 회복하기 위한 수단과, 상기 볼륨 ID 및 상기 발행 번호와 연관된 총 플레이 시간값에 상기 플레이 시간을 부가하기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 33

사용자가 분포된 애플리케이션 패키지(상기 볼륨)의 종류를 식별하기 위한 볼륨 ID, 발행된 순서로 각 종류의 볼륨에 부여되는 발행 번호, 및 애프리케이션에 대한 애플리케이션 ID를 볼륨 제어 데이터로 더 포함하는 분포 애플리케이션 패키지내에 포함되는 애플리케이션을 플레이하는 것을 허용하는 시스템에 있어서,

상기 애플리케이션을 플레이하는 클라이언트와,

통신 네트워크를 통해 상기 클라이언트를 제어하는 서버를 구비하고,

상기 클라이언트가 상기 볼륨 ID, 상기 발행 번호, 및 상기 애플리케이션 ID를 상기 서버에 전달하기 위한 수단을 구비하고 또한,

상기 서버가 상기 볼륨 ID, 상기 발행 번호, 및 상기 애플리케이션 ID와 연관된 예상 플레이 시간을 회복하기 위한 수단과, 상기 볼륨 ID 및 상기 발행 번호와 연관된 총 플레이 시간값에 상기 예상 플레이 시간을 부가하기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 34

사용자가 분포된 애플리케이션 패키지(상기 볼륨)의 종류를 식별하기 위한 볼륨 ID, 발행된 순서로 각 종류의 볼륨에 부여되는 발행 번호, 및 애플리케이션에 대한 애플리케이션 ID를 볼륨 제어 데이터로 더 포함하는 분포 애플리케이션 패키지내에 포함되는 애플리케이션을 플레이하는 것을 허용하는 시스템에 있어서,

상기 애플리케이션을 플레이하는 클라이언트와,

통신 네트워크를 통해 상기 클라리언트를 제어하는 서버를 구비하고,

상기 클라이언트 및 상기 서버가 상기 애플리케이션의 플레이 시간을 측정된 플레이 시간으로 대화식으로 측정하기 위한 수단을 구비하고, 또한

상기 서버가 상기 볼륨 ID 및 상기 발행 번호와 연관된 총 플레이 시간값에 상기 측정된 플레이 시간을 부가하기 위한 수단을 더 구비하는 것을 특징으로 하는 시스템.

청구항 35

제 34 항에 있어서,

플레이 시간을 대화식으로 측정하기 위한 상기 수단은 상기 서버의 타이머를 이용하기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 36

제 34 항에서 있어서,

플레이 시간을 대화식으로 측정하기 위한 상기 수단은 상기 클라이언트의 타이머를 이용하기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 37

사용자가 애플리케이션 데이터 및 제어 데이터를 포함하는 애플리케이션 패키지(볼륨)을 플레이하는 것을 허용하고, 상기 볼륨의 생성 이후에 제어 데이터 중 적어도 일부가 볼륨에 부가되는 시스템에 있어서,

상기 볼륨을 플레이하는 클라이언트와,

통신 네트워크를 통해 상기 클라이언트를 제어하는 서버를 구비하고, 여기서 상기 서버는 상기 서버의 비밀키를 저장하기 위한 수단을 구비하고, 상기 제어 데이터 중 적어도 일부는 상기 비밀키에 대응하는 공중키를 포함하고, 또한 상기 시스템이

의사 랜덤수를 발생하기 위해 상기 서버에 제공되는 수단과,

상기 의사 랜덤수를 저장하는 수단과,

상기 의사 랜덤수를 상기 클라이언트에 전송하기 위해 상기 서버에 제공되는 수단과,

상기 전송된 의사 랜덤수를 이용해 원하는 데이터를 암호화 데이터로 암호화 하기 위해 상기 클라이언트에 제공된 수단과,

상기 공중키를 사용해 상기 의사 랜덤수 및 상기 암호화 데이터로 구성된 연관 데이터를 이중-암호화 데이터로 암호화하기 위해 상기 클라이언트에 제공되는 수단과,

상기 이중-암호화 데이터를 상기 서버에 전달하기 위해 상기 클라이언트에 제공되는 수단과,

상기 비밀키를 사용해 상기 이중-암호화 데이터를 해독된 랜덤수 부분과 또 다른 해독 부분으로 구성되는 해독 데이터로 해독하기 위해 상기 서버에 제공되는 수단과,

상기 원하는 데이터를 구하도록 상기 전송된 랜덤수로 상기 또 다른 해독 부분을 해독하기 위해 상기 서버에 제공되는 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 38

제 37 항에 있어서,

상기 서버에 제공되고, 상기 또 다른 해독 부분을 해독하기 전에 활성화되고, 상기 해독된 랜덤수 부분이 상기 의사 랜덤수를 저장하기 위한 상기 수단에 저장된 상기 의사 랜덤수와 일치하지 않는다는 결정에 응답해, 다음 수단에 제어를 전하는 대신에 상기 클라이언트에 해독 실패를 알리는 수단을 더 구비하는 것을 특징으로 하는 시스템.

청구항 39

사용자가 분포된 애플리케이션 패키지(상기 볼륨)의 종류를 식별하기 위한 볼륨 ID, 발행된 순서로 각 종류의 볼륨에 부여되는 발행 번호, 및 애플리케이션 ID를 볼륨 제어 데이터로 더 포함하는 분포 애플리케이션 패키지내에 포함되는 애플리케이션을 플레이하는 것을 허용하는 시스템에 있어서,

애플리케이션 데이터를 이용함으로써 애플리케이션을 플레이하는 클라이언트와,

통신 네트워크를 통해 상기 클라이언트를 제어하는 서버를 구비하고,

상기 클라이언트가

상기 볼륨으로부터 암호키-암호화 애플리케이션 중 상기 하나(상기 암호키-암호화 애플리케이션)에 대해 상기 볼륨 ID, 상기 발행 번호, 및 애플리케이션 ID를 판독하여 상기 서버에 전달하는 수단을 구비하고,

상기 서버가

볼륨 데이터 도표에서 상기 볼륨 ID, 상기 발행 번호, 및 상기 애플리케이션 ID와 연관된 미터 필드의 값이 상기 보륨 ID, 상기 발행 번호, 및 상기 애플리케이션 ID와 연관된 제한값 필드의 값 이하인 경우에만 다음 단계로 진행되는 수단과,

상기 클라이언트가 디스플레이 장치에서 과도 제한을 상기 클라이언트에 알리는 메시지를 디스플레이하고, 그렇지 않은 경우 동작을 중단시키게 하는 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 40

사용자 분포된 애플리케이션 패키지(상기 볼륨)의 종류를 식별하기 위한 볼륨 ID, 발행된 순서로 각 종류의 볼륨에 부여되는 발행 번호, 애플리케이션 ID, 및 각 애플리케이션의 플레이를 제한하도록 각 애플리케이션 ID와 연관되는 제한값을 볼륨 제어 데이터로 더 포함하는 분포 애플리케이션 패키지내에 포함되는 애플리케이션을 플레이하는 것을 허용하는 시스템에 있어서,

애플리케이션 데이터를 이용함으로써 애플리케이션을 플레이하는 클라이언트와,

통신 네트워크를 통해 상기 클라이언트를 제어하는 서버를 구비하고,

상기 클라이언트가

상기 볼륨 ID, 상기 발행 번호, 및 암호키-암호화 애플리케이션 중 상기 하나(상기 암호키-암호화 애플리케이션)에 대한 애플리케이션 ID, 및 상기 애플리케이션 ID와 연관된 제한값을 판독하여 상기 서버에 전달하는 수단을 구비하고,

상기 서버가

볼륨 데이터 도표에서 상기 볼륨 ID, 상기 발행 번호, 및 상기 애플리케이션 ID와 연관된 미터 필드의 값이 상기 제한값 이하인 경우에만 다음 단계로 진행되는 수단과,

상기 클라이언트가 디스플레이 장치에서 과도 제한을 상기 클라이언트에 알리는 메시지를 디스플레이하고, 그렇지 않은 경우 동작을 중단시키게 하는 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 41

제 39 항에 있어서,

상기 제한값이 유효 날짜 및 시간, 허용가능한 만기 날짜 및 시간, 플레이 시간의 최대량, 또한 허용가능한 억세스 카운트 중 하나인 것을 특징으로 하는 시스템.

청구항 42

제 29 항, 제 33 항, 및 제 34 항 중 한 항에 있어서,

상기 서버에 전달하는 상기 수단이 상기 볼륨 ID , 상기 발행 번호, 및 상기 애플리케이션 ID 중 적어도 하나를 암호화하기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 43

인증된 사용자가 애플리케이션을 플레이할 수 있는 시스템에서 분포된 애플리케이션 패키지에 포함되는 애플리케이션 중 원하는 것을 플레이하는 것을 허용하고, 상기 애플리케이션 패키지(상기 볼륨)가 상기 볼륨의 애플리케이션과 상기 볼륨에 지정된 모드 코드를 포함하는 볼륨 제어 데이터를 포함하는 방법에 있어서,

상기 원하는 애플리케이션과 연관된 상기 모드 코드 중 하나에 의해 지정되는 소정의 플레이 모드 중 하나를 사용하도록 결정하는 단계와,

상기 지정된 플레이 모드로 상기 원하는 애플리케이션을 플레이하는 단계를 구비하는 것을 특징으로 하는 방법.

청구항 44

제 43 항에 있어서,

상기 모드 코드에, 사용을 제한하도록 사용되는 각 제한값에 대응하는 적어도 하나의 제한-부착 플레이 모드와 무료 플레이 모드를 나타내는 값을 포함하는 단계를 더 구비하는 것을 특징으로 하는 방법.

청구항 45

제 44 항에 있어서,

상기 원하는 애플리케이션을 플레이하는 상기 단계가

상기 원하는 애플리케이션과 연관된 상기 모드 코드 중 하나가 상기 무료 플레이 모드를 나타내는 값을 포함한다는 결정에 응답해, 상기 원하는 애플리케이션을 간단히 플레이하는 단계를 구비하는 것을 특징으로 하는 방법.

청구항 46

제 44 항에 있어서,

상기 원하는 애플리케이션을 플레이하는 상기 단계가

상기 원하는 애플리케이션과 연관된 상기 모드 코드 중 하나가 상기 적어도 하나의 제한-부착 플레이 모드를 나타내는 값을 포함한다는 결정에 응답해, 상기 제한값에 이르면 상기 원하는 애플리케이션을 플레이하는 대신에 상기 값 중 하나에 연관된 제한값에 이른다는 취지로 메시지를 디스플레이하는 단계를 구비하는 것을 특징으로 하는 방법.

청구항 47

제 43 항에 있어서,

상기 볼륨 제어 데이터가 볼륨 ID, 발행 번호, 및 상기 각 애플리케이션에 대한 애플리케이션 ID를 더 포함하고, 소정의 플레이 모드 중 하나를 사용하도록 결정하는 단계가,

상기 애플리케이션 ID를 사용함으로써 대응하는 제한값 및 상기 원하는 애플리케이션과 연관된 상기 모드 코드 중 하나를 구하는 단계와,

상기 모드 코드 중 하나를 상기 볼륨 ID, 상기 발행 번호, 및 상기 애플리케이션 ID와 연관된 미터 미터값과 비교하는 단계를 구비하는 것을 특징으로 하는 방법.

청구항 48

제 45 항에 있어서,

상기 각 애플리케이션이 암호키로 각각 암호화되고, 상기 볼륨 제어 데이터가 상기 암호키의 사용자 공중키-암호화 버전(공중키-암호화 버전 암호키)을 포함하고, 상기 원하는 애플리케이션을 간단히 플레이하는 상기 단계가

상기 볼륨으로부터 상기 사용자 공중키-암호화 암호키를 판독하는 단계와,

상기 사용자 공중키에 대응하는 사용자의 비밀키를 구하는 단계와,

상기 암호키를 구하도록 상기 사용자 비밀키로 상기 사용자 공중키-암호화 암호키를 해독하는 단계와,

상기 구해진 암호키로 상기 원하는 애플리케이션을 해독하는 단계를 구비하는 것을 특징으로 하는 방법.

청구항 49

인증된 사용자가 분포된 애플리케이션 패키지에 포함되는 애플리케이션 중 원하는 것을 플레이하는 것을 허용하고, 상기 애플리케이션 패키지(상기 볼륨)가 상기 볼륨의 애플리케이션과 상기 볼륨에 지정된 모드 코드를 포함하는 볼륨 제어 데이터를 포함하는 시스템에 있어서,

상기 원하는 애플리케이션과 연관된 상기 모드 코드 중 하나에 의해 지정되는 소정의 플레이 모드 중 하나를 사용하도록 결정하는 단계와,

상기 지정된 플레이 모드로 상기 원하는 애플리케이션을 플레이하는 단계를 구비하는 것을 특징으로 하는 시스템.

청구항 50

제 49 항에 있어서,

상기 모드 코드에, 사용을 제한하도록 사용되는 각 제한값에 대응하는 적어도 하나의 제한-부착 플레이 모드와 무료 플레이 모드를 나타내는 값을 포함하기 위한 수단을 더 구비하는 것을 특징으로 하는 시스템.

청구항 51

제 50 항에 있어서,

상기 원하는 애플리케이션을 플레이하기 위한 수단이

상기 원하는 애플리케이션과 연관된 상기 모드 코드 중 하나가 상기 무료 플레이 모드를 나타내는 값을 포함한다는 결정에 응답해, 상기 원하는 애플리케이션을 간단히 플레이하기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 52

제 50 항에 있어서,

상기 원하는 애플리케이션을 플레이하기 위한 수단이

상기 원하는 애플리케이션과 연관된 상기 모드 코드 중 하나가 상기 적어도 하나의 제한-부착 플레이 모드를 나타내는 값을 포함한다는 결정에 응답해, 상기 제한값에 이르면 상기 원하는 애플리케이션을 플레이하는 대신에 상기 값 중 하나에 연관된 제한값에 이른다는 취지로 메시지를 디스플레이하기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 53

제 49 항에 있어서

상기 볼륨 제어 데이터가 볼륨 ID, 발행 번호, 및 상기 각 애플리케이션에 대한 애플리케이션 ID를 더 포함하고, 소정의 플레이 모드 중 하나를 사용하도록 결정하기 위한 상기 수단이

상기 애플리케이션 ID를 사용함으로써 대응하는 제한값 및 상기 원하는 애플리케이션과 연관된 상기 모드 코드 중 하나를 구하기 위한 수단과,

상기 모드 코드 중 하나를 상기 볼륨 ID, 상기 발행 번호, 및 상기 애플리케이션 ID와 연관된 미터 미터 값과 비교하기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 54

제 51 항에 있어서,

상기 각 애플리케이션이 암호키로 각각 암호화되고, 상기 볼륨 제어 데이터가 상기 암호키의 사용자 공중키-암호화 버전(공중키-암호화 버전 암호키)을 포함하고, 상기 원하는 애플리케이션을 간단히 플레이하기 위한 수단이

상기 볼륨으로부터 상기 사용자 공중키-암호화 암호키를 판독하기 위한 수단과,

상기 사용자 공중키에 대응하는 사용자의 비밀키를 구하기 위한 수단과,

상기 암호키를 구하도록 상기 사용자 비밀키로 상기 사용자 공중키-암호화 암호키를 해독하기 위한 수단과,

상기 구해진 암호키로 상기 원하는 애플리케이션을 해독하기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 55

인증된 사용자가 애플리케이션을 플레이할 수 있는 클라이언트 및 통신 네트워크를 통해 상기 클라이언트와 연결된 서버를 구비하는 시스템에서 분포된 애플리케이션 패키지에 포함되는 애플리케이션 중 원하는 것을 플레이하는 것을 허용하고, 상기 애플리케이션 패키지(이후 상기 볼륨이라 칭하여지는)가 상기 볼륨의 애플리케이션과 상기 볼륨에 지정된 모드 코드를 포함하는 볼륨 제어 데이터를 포함하는 방법에 있어서,

상기 클라이언트가 상기 원하는 애플리케이션과 연관된 상기 모드 코드 중 하나에 의해 지정되는 소정의 플레이 모드 중 하나를 사용하도록 결정하는 단계와,

상기 클라이언트와 상기 서버간의 협력에 상기 지정된 플레이 모드로 상기 원하는 애플리케이션을 플레이 하는 단계를 구비하는 것을 특징으로 하는 방법.

청구항 56

제 55 항에 있어서,

상기 모드 코드 각각에, 무료 플레이 모드, 유료 플레이 모드, 및 적어도 하나의 제한-부착 플레이 모드 중 하나를 나타내는 값을 포함하는 단계를 더 구비하고, 상기 볼륨 제어 데이터가 상기 적어도 하나의 제한-부착 플레이 모드 각각에 연관된 제한값을 더 포함하는 것을 특징으로 하는 방법.

청구항 57

제 55 항 또는 제 56 항 중 한 항에 있어서,

상기 볼륨 제어 데이터가 볼륨 ID, 발행 번호, 및 상기 각 애플리케이션에 대한 애플리케이션 ID를 더 포함하고, 상기 원하는 애플리케이션을 상기 지정된 플레이 모드로 플레이하는 상기 단계가 상기 지정된 애플리케이션을 간단히 플레이하는 애플리케이션 플레이 단계를 포함하는 것을 특징으로 하는 방법.

청구항 58

제 57 항에 있어서,

분포된 애플리케이션 패키지에 포함되는 상기 각 플레이 암호키로 암호화 되고, 상기 볼륨 제어 데이터가 상기 암호키의 사용자 공중키-암호화 버전(공중키-암호화 버전 암호키)을 포함하고, 또한 상기 애플리케이션 플레이 단계가

상기 볼륨으로부터 상기 사용자 공중키-암호화 암호키를 판독하는 단계와,

상기 사용자 공중키에 대응하는 사용자의 비밀키를 구하는 단계와,

상기 암호키를 구하도록 상기 사용자 비밀키로 상기 사용자 공중키-암호화 암호키를 해독하는 단계와,

상기 구해진 암호키로 상기 원하는 애플리케이션을 해독하는 단계를 구비하는 것을 특징으로 하는 방법.

청구항 59

제 57 항에 있어서,

분포된 애플리케이션 패키지에 포함되는 상기 각 플레이어 암호키로 암호화 되고, 상기 볼륨 제어 데이터가 상기 암호키의 사용자 공중키-암호화 버전(공중키-암호화 버전 암호키)을 포함하고, 또한 상기 애플리케이션 플레이 단계가

상기 서버에서,

상기 볼륨 ID를 이용해 암호키를 회복하는 단계와,

상기 볼륨 ID 및 상기 발행 번호와 연관된 사용자 공중키를 회복하는 단계와,

의사 랜덤수와 상기 사용자 공중키를 사용해 상기 암호키를 이중 암호화 데이터로 이중-암호화하는 단계와,

상기 이중-암호화된 데이터를 상기 클라이언트에 전달하는 단계와,

상기 클라이언트에서,

상기 사용자 공중키에 대응하는 사용자 비밀키를 구하는 단계와,

상기 사용자 비밀키로 상기 이중-암호화된 데이터를 해독하여 상기 암호키를 구하는 단계와,

상기 구해진 암호키로 상기 원하는 애플리케이션을 해독하는 단계를 구비하는 것을 특징으로 하는 방법.

청구항 60

제 57 항에 있어서,

상기 원하는 애플리케이션을 플레이하는 상기 단계가 상기 애플리케이션 플레이 단계에 앞서 실행되는,

상기 서버가 상기 원하는 애플리케이션과 연관된 기대 플레이 시간을 회복하는 단계와,

상기 기대 플레이 시간을 상기 클라이언트의 디스플레이 장치에 디스플레이 하는 단계를 더 구비하는 것을 특징으로 하는 방법.

청구항 61

제 57 항에 있어서,

상기 원하는 애플리케이션을 플레이하는 상기 단계가

상기 애플리케이션 플레이 단계의 기간을 측정된 플레이 시간으로 측정하는 단계와,

총 플레이 시간량을 구하도록 상기 모드 코드와 연관된 플레이 시간 미터에 상기 측정된 플레이 시간을 부가하는 단계와,

상기 애플리케이션 플레이 단계 이후에 상기 측정된 플레이 시간과 상기 총 플레이 시간량을 상기 클라이

언트의 디스플레이 장치에 디스플레이하는 단계를 더 구비하는 것을 특징으로 하는 방법.

청구항 62

제 61 항에 있어서,

기간을 측정하는 상기 단계와 상기 서버의 타이머를 이용함으로써 상기 플레이 시간을 측정하는 단계를 구비하는 것을 특징으로 하는 방법.

청구항 63

제 61 항에 있어서,

기간을 측정하는 상기 단계와 상기 클라이언트의 타이머를 이용하여 상기 플레이 시간을 측정하는 단계를 구비하는 것을 특징으로 하는 방법.

청구항 64

제 57 항에 있어서,

소정의 플레이 모드 중 하나를 사용하도록 결정하는 상기 단계가 상기 원하는 애플리케이션과 연관된 상기 모드 코드 중 하나가 상기 유료 플레이 모드를 나타내는 값을 포함하면 상기 유료 플레이 모드를 사용하도록 결정하는 것을 구비하고, 상기 원하는 애플리케이션을 플레이하는 상기 단계가

상기 클라이언트가 상기 사용자의 신용 카드 번호를 구하여 상기 서버에 전달하는 단계와,

상기 번호의 신용 카드가 연관된 신용 카드 회사를 참고하여 유효한 것으로 발견되는 경우에만 다음 단계로 진행되는 단계와,

상기 애플리케이션 플레이 단계의 기간 측정을 근거로 결정된 플레이에 대한 요금 청구와 총 플레이 청구량을 상기 애플리케이션 플레이 단계 이후에 상기 클라이언트의 디스플레이 장치상에 디스플레이하는 단계와,

상기 서버가 상기 신용 카드 번호에 상기 플레이에 대해 청구하는 단계를 구비하는 것을 특징으로 하는 방법.

청구항 65

제 64 항에 있어서,

상기 원하는 애플리케이션 플레이하는 상기 단계가 상기 애플리케이션 플레이 단계 이전에,

상기 디스플레이 장치상에 예상 요금 청구 및 총 예상 청구량을 상기 애플리케이션 플레이 단계 이전에 디스플레이하는 단계와,

사용자에게 상기 원하는 애플리케이션을 플레이할 것인가 여부를 결정하게 하는 단계를 더 구비하는 것을 특징으로 하는 방법.

청구항 66

제 64 항에 있어서,

상기 클라이언트가 상기 사용자의 신용 카드 번호를 구하여 상기 서버에 전달하는 상기 단계가

상기 서버에서,

의사 랜덤수를 발생하는 단계와,

상기 의사 랜덤수를 메모리에 저장하는 단계와.

상기 의사 랜덤수를 상기 클라이언트에 전송하는 단계와,

상기 클라이언트에서,

상기 사용자에게 상기 신용 카드 번호를 입력하도록 촉구하는 단계와,

상기 전송된 랜덤수 및 상기 봄릅 제어 데이터에 포함되는 서버의 공중키를 사용해 상기 신용 카드 번호를 먼저 이중-부호화 번호로 이중-암호화 하는 단계와,

상기 이중-암호화 번호를 상기 서버에 전달하는 단계와.

상기 서버에서

서버의 비밀키를 사용해 상기 이중-암호화 번호를 해독 랜덤수 및 또 다른 해독 데이터로 해독하는 단계와,

상기 신용 카드 번호를 구하도록 상기 전송된 랜덤수로 상기 또 다른 해독 데이터를 해독하는 단계를 구비하는 것을 특징으로 하는 방법.

청구항 67

제 66 항에 있어서,

상기 클라이언트가 상기 사용자의 신용 카드 번호를 구하여 상기 서버에 전달하는 상기 단계가 상기 또 다른 암호화 데이터를 해독하는 상기 단계 이전에 실행되는,

상기 해독된 랜덤수가 상기 메모리에 저장된 상기 의사 랜덤수와 일치하는 경우에만 다음 단계로 진행되는 단계와,

해독 실패를 알리고 그렇지 않은 경우에는 동작을 중단하는 메시지를 디스플레이하는 단계를 더 구비하는 것을 특징으로 하는 방법.

청구항 68

제 57 항에 있어서,

상기 원하는 애플리케이션과 연관된 상기 모드 코드 중 하나가 상기 적어도 하나의 제한-부착 플레이 모드 중 하나를 나타내는 값을 포함하면 소정의 플레이 모드 중 하나를 사용하도록 결정하는 것을 구비하고, 상기 원하는 애플리케이션을 플레이하는 상기 단계가,

볼륨 데이터 도표에서 상기 볼륨 ID, 상기 발행 번호, 및 상기 원하는 애플리케이션의 애플리케이션 ID에 의해 식별되는 기록내의 상기 원하는 애플리케이션과 연관되는 상기 모드 코드 중 하나와 연관된 미터값이 상기 모드 코드와 연관된 제한값에 이른다는 결정에 응답해, 상기 애플리케이션 플레이 단계를 실행하는 대신에 상기 클라이언트의 디스플레이 장치에 과도 제한을 알리는 메시지를 디스플레이하는 단계를 구비하는 것을 특징으로 하는 방법.

청구항 69

제 68 항에 있어서,

상기 제한값이 유효 날짜 및 시간, 허용가능한 만기 날짜 및 시간, 플레이 시간의 최대량, 또한 허용가능한 억세스 카운트 중 하나인 것을 특징으로 하는 방법.

청구항 70

서버와 제휴하여 소정의 플레이 모드 중 하나로 분포된 애플리케이션 패키지를 플레이하고, 애플리케이션 패키지가 시스템 및 서버의 동작을 제어하는데 사용되도록 볼륨 제어 데이터 및 적어도 하나의 애플리케이션 각각에 대해 암호키(K-암호화 데이터 세트)로 암호화된 데이터 세트를 포함하고, 볼륨 제어 데이터가 상기 플레이 모드를 정의하는 모드 코드를 포함하는 시스템에 있어서,

사용자가 상기 볼륨의 상기 적어도 하나의 애플리케이션 중 하나를 선택하는 것을 허용하기 위한 수단과,

상기 선택된 애플리케이션에 지정된 상기 모드 코드 중 하나와 연관되는 상기 소정의 플레이 모드 중 하나를 사용하도록 결정하기 위한 수단과,

상기 서버와 제휴하여 상기 선택된 플레이 모드로 상기 선택된 애플리케이션을 플레이하기 위한 수단을 구비하는 것을 특징으로 하는 시스템

청구항 71

제 70 항에 있어서,

상기 각 모드 코드가 무료 플레이 모드, 유료 플레이 모드, 및 적어도 하나의 제한-부착 플레이 모드에 대한 값 중 하나를 포함하는 것을 특징으로 하는 시스템.

청구항 72

제 70 항에 있어서,

상기 볼륨 제어 데이터가 볼륨 ID, 발행 번호, 및 상기 각 애플리케이션에 대한 애플리케이션 ID를 더 포함하고, 상기 선택된 플레이 모드로 상기 선택된 애플리케이션을 플레이하기 위한 상기 수단이 적어도

상기 서버에 상기 볼륨 ID, 발행 번호, 및 애플리케이션 ID, 그리고 상기 선택된 애플리케이션과 연관된 상기 모드 코드를 전달함으로써 상기 서버를 상기 선택된 플레이 모드로 설정하기 위한 수단과,

상기 지정된 애플리케이션을 간단히 플레이하기 위한 애플리케이션 플레이 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 73

제 72 항에 있어서,

상기 볼륨 제어 데이터가 사용자의 공중키-암호화 암호키를 더 포함하고, 상기 애플리케이션 플레이 수단이

상기 볼륨으로부터 상기 사용자 공중키-암호화 암호키를 판독하기 위한 수단과,

상기 사용자의 공중키에 대응하는 사용자의 비밀키를 구하기 위한 수단,

상기 암호키를 구하도록 상기 사용자의 비밀키로 상기 사용자의 공중키-암호화 암호키를 해독하기 위한 수단과,

상기 구해진 암호키로 상기 선택된 애플리케이션의 K-암호화 데이터 세트를 해독하기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 74

제 73 항에 있어서,

상기 사용자의 공중키-암호화 암호키를 해독하기 위한 수단과, K-암호화 데이터 세트를 해독하기 위한 수단이 집적 회로로 실현되는 것을 특징으로 하는 시스템.

청구항 75

제 72 항에 있어서,

상기 애플리케이션 플레이 수단이

상기 서버로부터 이중-암호화 데이터를 수신하기 위한 수단과,

상기 사용자의 공중키에 대응하는 사용자의 비밀키를 구하기 위한 수단과,

상기 사용자의 비밀키로 상기 이중-암호화 데이터를 해독함으로서 상기 암호키를 구하기 위한 수단과,

상기 구해진 암호키로 상기 선택된 애플리케이션의 K-암호화 데이터 세트를 해독하기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 76

제 75 항에 있어서,

상기 암호키를 구하기 위한 상기 수단과 K-암호화 데이터 세트를 해독하기 위한 수단이 집적 회로로 실현되는 것을 특징으로 하는 시스템.

청구항 77

제 74 항 또는 제 76 항에 있어서,

상기 집적 회로가 사용자의 비밀키를 구하기 위한 상기 수단에 통합되는 것을 특징으로 하는 시스템.

청구항 78

제 73 항에 있어서,

하나를 사용하도록 결정하기 위한 상기 수단이 무료 플레이 모드를 사용하도록 결정하기 위한 수단을 구비하고, 상기 선택된 애플리케이션을 플레이하기 위한 상기 수단이 상기 애플리케이션 플레이 수단 이전에,

상기 서버로부터 데이터를 수신하기 위한 수단과,

상기 데이터를 상기 선택된 애플리케이션에 대한 기대 플레이 시간으로 디스플레이하기 위한 수단을 더 구비하는 것을 특징으로 하는 시스템.

청구항 79

제 73 항에 있어서,

상기 소정의 플레이 모드 중 하나를 사용하도록 결정하기 위한 상기 수단이 무료 플레이 모드를 사용하도록 결정하는 수단을 구비하고, 상기 선택된 애플리케이션을 플레이하기 위한 수단이

상기 서버가 상기 애플리케이션 플레이 시간의 동작 주기 데이터를 측정된 플레이 시간으로 구하도록 하기 위한 수단과,

상기 서버로부터 제 1 및 제 2 데이터를 수신하기 위한 수단과,

상기 애플리케이션 플레이 수단에 의한 동작이 완료된 직후에 상기 제 1 및 제 2 데이터를 상기 측정된 플레이 시간 및 총 플레이 시간량으로 디스플레이하기 위한 수단을 더 구비하는 것을 특징으로 하는 시스템.

청구항 80

제 79 항에 있어서,

상기 서버가 상기 동작 주기 데이터를 구하도록 하기 위한 상기 수단이 상기 서버의 타이머를 사용하도록 상기 애플리케이션 플레이 수단에 의한 동작의 시작 및 끝을 상기 서버에 알리기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 81

제 79 항에 있어서,

상기 서버가 동작 주기 데이터를 구하도록 하기 위한 상기 수단이

상기 애플리케이션 플레이 수단의 상기 동작 주기를 측정하기 위한 수단과,

상기 총 플레이 시간량의 계산에서 사용되도록 상기 동작 주기를 상기 서버에 전달하기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 82

제 72 항에 있어서,

하나를 사용하도록 결정하기 위한 상기 수단이 유료 플레이 모드를 사용하도록 결정하기 위한 수단을 구

비하고, 상기 선택된 애플리케이션을 플레이하기 위한 상기 수단이

상기 사용자의 신용 카드 번호를 구하여 상기 서버에 전달하기 위한 수단과,

결과가 긍정적인 경우에만 다음 처리 과정을 시작하도록 상기 서버로부터의 상기 신용 카드 확인 결과에 응답하는 수단과,

상기 애플리케이션 플레이 수단의 동작 이후에 상기 애플리케이션 플레이 수단의 측정된 플레이 시간을 근거로 결정되는 플레이에 대한 청구 및 총 플레이 청구량을 디스플레이 하기 위한 수단을 더 구비하는 것을 특징으로 하는 시스템.

청구항 83

제 82 항에 있어서,

상기 선택된 애플리케이션을 플레이하기 위한 상기 수단이

예상 청구 및 총 예상 청구량을 디스플레이하고 사용자에게 상기 선택된 애플리케이션을 플레이할 것인가 여부를 결정하게 하도록 상기 애플리케이션 플레이 수단의 동작 이전에 활성화되는 수단을 더 구비하는 것을 특징으로 하는 시스템.

청구항 84

제 82 항에 있어서,

상기 분포된 애플리케이션 패키지의 상기 볼륨 제어 데이터가 서버의 공중키를 더 포함하고, 상기 사용자의 신용 카드 번호를 구하여 상기 서버에 전달하기 위한 상기 수단이

상기 사용자에게 상기 신용 카드 번호를 입력하도록 촉구하기 위한 수단과,

상기 서버로부터 랜덤수를 수신하기 위한 수단과,

상기 볼륨으로부터 상기 서버의 공중키를 구하기 위한 수단과,

상기 랜덤수 및 상기 서버의 공중키를 사용해 상기 신용 카드 번호를 먼저 이중-암호화 데이터로 이중-암호화하기 위한 수단과,

상기 이중-암호화 번호를 상기 서버에 전달하기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 85

제 84 항에 있어서,

상기 클라이언트가 상기 사용자의 신용 카드 번호를 구하여 상기 서버에 전달하기 위한 상기 수단이

다음 처리 과정을 시작하도록 상기 서버로부터의 랜덤수 점검의 긍정적인 결과에 응답하는 수단과,

상기 선택된 애플리케이션에 대한 동작을 중단하고 상기 랜덤수 점검에서 실패를 나타내는 메시지를 디스플레이하도록 상기 서버로부터의 상기 랜덤수 점검의 부정적인 결과에 응답하는 수단을 더 구비하는 것을 특징으로 하는 시스템.

청구항 86

제 72 항에 있어서,

하나를 사용하도록 결정하기 위한 상기 수단이 제한-부착 플레이 모드를 사용하도록 결정하기 위한 수단을 구비하고,

상기 서버에 전달하기 위한 수단이 상기 모드 코드와 연관된 제한값을 전송하는 것을 포함하고, 상기 선택된 애플리케이션을 플레이하기 위한 상기 수단이

상기 모드 코드와 연관된 제한값에 이르렀는가 여부를 나타내는 제한 점검 결과를 상기 서버로부터 수신하도록 상기 애플리케이션 플레이 수단의 동작에 앞서 동작되는 수단과,

다음 동작을 시작하도록 상기 결과의 과도 제한 경우에 응답하는 수단을 더 구비하는 것을 특징으로 하는 시스템.

청구항 87

제 86 항에 있어서,

상기 제한값이 유효 날짜 및 시간, 허용가능한 만기 날짜 및 시간, 플레이 시간의 최대량, 또한 허용가능한 억세스 카운트 중 하나인 것을 특징으로 하는 시스템.

청구항 88

소정의 플레이 모드 중 하나로 분포된 애플리케이션 패키지를 플레이하는 클라이언트 장치를 통신 네트워크를 통해 제어하고, 애플리케이션 패키지가 시스템 및 클라이언트의 동작을 제어하는데 사용되도록 볼륨 제어 데이터 및 적어도 하나의 애플리케이션 각각에 대해 암호키(K-암호화 데이터 세트)로 암호화된 데이터 세트를 포함하고, 볼륨 제어 데이터가 볼륨 ID, 발행 번호, 상기 각 애플리케이션에 대한 애플리케이션 ID, 및 상기 볼륨에 대한 모드 코드나 상기 애플리케이션에 대한 모드 코드를 포함하는 시스템에 있어서,

각 볼륨에 대해 상기 볼륨 ID, 상기 발행 번호, 상기 볼륨에 대한 상기 모드 코드, 및 상기 애플리케이션

ID 그리고 상기 애플리케이션의 각각에 대한 상기 모드 코드를 저장하기 위한 볼륨 데이터 도표와,

상기 클라이언트로부터 서비스 요구, 볼륨 ID, 발행 번호, 애플리케이션 ID, 및 모드 코드와 다른 데이터를 수신하기 위한 수단과,

상기 볼륨 ID 및 상기 발행 번호에 의해 식별되는 기록의 적절한 필드에 상기 수신된 애플리케이션 ID, 상기 수신된 모드 코드, 및 다른 데이터를 저장하기 위한 수단과,

상기 볼륨 데이터 도표에 상기 기록을 부가하고 상기 기록의 관련 필드에 상기 수신된 애플리케이션 ID와 모드 코드, 그리고 상기 다른 데이터를 저장하도록 상기 볼륨 데이터 도표에서 상기 볼륨 ID 및 상기 발행 번호에 의해 식별되는 기록이 없다는 결정에 응답하는 수단과,

상기 수신된 모드 코드와 연관된 플레이 모드를 지지하는 수단에 제어를 순차적으로 전달하게 결정하도록 상기 수신된 모드 코드를 근거로 동작되는 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 89

제 88 항에 있어서,

플레이 모드를 지지하기 위한 상기 수단이 적어도 상기 수신된 애플리케이션 ID에 의해 식별된 애플리케이션을 간단히 실행하도록 클라이언트의 애플리케이션 플레이 수단을 지지하기 위한 수단을 구비하고, 상기 클라이언트의 상기 애플리케이션 플레이 수단을 지지하기 위한 상기 수단이

주어진 볼륨 ID를 대응하는 암호키와 연관시키기 위한 제 1 수단과,

주어진 볼륨 ID 및 발행 번호를 대응하는 사용자의 공중키와 연관시키기 위한 수단과,

상기 제 1 수단으로부터 상기 수신된 볼륨 ID와 연관되는 암호키를 회복하기 위한 수단과,

상기 제 2 수단으로부터 상기 수신된 볼륨 ID 및 발행 번호와 연관되는 사용자 공중키를 회복하기 위한 수단과,

의사 랜덤수와 상기 사용자 공중키를 사용해 상기 암호키를 이중 암호화 데이터로 이중-암호화 하기 위한 수단과,

상기 이중-암호화 데이터를 상기 클라이언트에 전달하기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 90

제 89 항에 있어서,

각 애플리케이션 종류에 대한 데이터를 저장하기 위한 애플리케이션 데이터 도표를 더 구비하고, 상기 수신된 모드 코드가 무료 플레이 모드를 정의하고, 상기 수신된 모드 코드와 연관된 플레이 모드를 지지하기 위한 상기 수단이

상기 애플리케이션 데이터 도표로부터 상기 수신된 애플리케이션 ID와 연관된 기대 플레이 시간을 회복하도록 상기 클라이언트의 애플리케이션 플레이 수단을 지지하기 위한 상기 수단의 동작 이전에 활성화되는 수단과,

상기 기대 플레이 시간을 상기 클라이언트에 전달하기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 91

제 89 항에 있어서,

상기 수신된 모드 코드가 무료 플레이 모드를 정의하고, 상기 수신된 모드 코드와 연관된 플레이 모드를 지지하기 위한 상기 수단이

애플리케이션 플레이의 기간을 측정된 플레이 시간으로 측정하기 위한 수단과,

총 플레이 시간량을 구하도록 상기 볼륨 데이터 도표에서 상기 수신된 모드 코드와 연관되는 플레이 시간 미터에 상기 측정된 플레이시간을 부가하기 위한 수단과,

상기 측정된 플레이 시간 및 상기 총 플레이 시간량을 상기 클라이언트에 전달하기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 92

제 91 항에 있어서,

기간을 측정하기 위한 상기 수단이

타이머를 시작하도록 상기 클라이언트의 상기 애플리케이션 플레이 수단에 의한 동작의 시작 통보에 응답하는 수단과,

상기 타이머를 중단시키도록 상기 동작의 종료 통보에 응답하는 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 93

제 91 항에 있어서,

기간을 측정하기 위한 상기 수단이

상기 클라이언트로부터 측정된 기간을 수신하기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 94

제 88 항에 있어서,

상기 수신된 모드 코드가 유료 플레이 모드를 정의하고, 상기 수신된 모드 코드와 연관된 플레이 모드를 지지하기 위한 상기 수단이

상기 서버로부터 상기 사용자의 신용 카드 번호를 수신하기 위한 수단과,

상기 클라이언트에게 무효임을 알리고 플레이 모드를 지지하기 위한 수단의 동작을 중단하도록 상기 신용 카드 번호의 확인으로부터 상기 신용 카드 번호가 유효하지 않다는 결정에 응답하는 수단과,

상기 클라이언트에게 유효함을 알리고 다음 동작으로 진행되도록 상기 신용 카드 번호의 상기 확인으로부터 상기 신용 카드 번호가 유효하다는 결정에 응답하는 수단과,

상기 신용 카드 번호에 상기 플레이에 대해 청구하기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 95

제 94 항에 있어서,

상기 수신된 모드 코드와 연관된 플레이 모드를 지지하기 위한 상기 수단이

상기 수신된 애플리케이션 ID를 사용함으로써 상기 애플리케이션 데이터 도표로부터 예상 청구를 회복하도록 상기 클라이언트의 상기 애플리케이션 플레이 수단 동작 이전에 활성화되는 수단과,

상기 수신된 모드 코드에 의존해 애플리케이션 ID 또는 상기 수신된 볼륨 ID와 연관된 청구 미터값 및 상기 예상 청구의 합을 계산하기 위한 수단과,

상기 예상 청구 및 상기 합을 상기 클라이언트에 전달하도록 상기 애플리케이션 플레이 수단 동작 이전에 동작되는 수단과,

플레이 모드를 지지하기 위한 상기 수단을 중단하도록 중단 메시지의 수신에 응답하는 수단을 더 구비하는 것을 특징으로 하는 시스템.

청구항 96

제 94 항에 있어서,

상기 서버로부터 상기 사용자의 신용 카드 번호를 수신하기 위한 상기 수단이

의사 랜덤수를 발생하기 위한 수단과,

상기 의사 랜덤수를 메모리에 저장하기 위한 수단과,

상기 의사 랜덤수를 상기 클라이언트에 전송하기 위한 수단과,

상기 클라이언트로부터 이중-암호화 데이터를 대기하기 위한 수단과,

서버의 비밀키를 구하기 위한 수단과,

상기 서버의 비밀키를 사용해 상기 이중-암호화 수를 해독된 랜덤수 및 또 다른 해독 데이터로 해독하기 위한 수단과,

상기 신용 카드 번호를 구하도록 상기 전송된 랜덤수로 상기 또 다른 암호화 데이터를 해독하기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 97

제 96 항에 있어서,

사용자의 비밀키를 구하기 위한 상기 수단이 상기 사용자의 휴대용 메모리로부터 상기 사용자 비밀키를 판독하기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 98

제 96 항에 있어서,

상기 서버로부터 상기 사용자의 신용 카드 번호를 수신하기 위한 상기 수단이

상기 클라이언트에 인에이블 메시지를 전달하여 다음 동작으로 진행되도록 상기 또 다른 데이터 해독에 앞서 이루어지는, 상기 해독된 랜덤수가 상기 메모리에 저장된 상기 의사 랜덤수와 일치한다는 결정에 응답하는 수단과,

상기 클라이언트에 디스에이블 메시지를 전달하여 상기 플레이 모드를 지지하는 것을 중단하도록 상기 또 다른 데이터 해독에 앞서 이루어지는, 상기 해독된 랜덤수가 상기 메모리에 저장된 상기 의사 랜덤수와 일치하지 않는다는 결정에 응답하는 수단을 더 구비하는 것을 특징으로 하는 시스템.

청구항 99

제 88 항에 있어서,

상기 수신된 모드 코드가 제한-부착 플레이 모드를 정의하고,

서비스 요구를 수신하기 위한 수단이 상기 모드 코드와 연관된 제한값을 더 수신하고, 상기 수신된 모드 코드와 연관된 플레이 모드를 지지하기 위한 상기 수단이

상기 볼륨 데이터 도표에서 상기 모드 코드와 연관된 소프트웨어 미터값이 상기 제한값 이하인 경우에만 다음 동작으로 진행되기 위한 수단과,

상기 볼륨 데이터 도표에서 상기 모드 코드와 연관된 소프트웨어 미터값이 상기 제한값 이하가 아닌 경우 상기 클라이언트에 과도 제한을 알리는 메시지를 전달하여 상기 수신된 모드 코드와 연관된 플레이 모드를 지지하기 위한 상기 수단의 동작을 중단하기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 100

제 99 항에 있어서,

상기 제한값이 유효 날짜 및 시간, 허용가능한 만기 날짜 및 시간, 플레이 시간의 최대량, 또한 허용가능한 억세스 카운트 중 하나인 것을 특징으로 하는 시스템.

청구항 101

제 54 항, 제 73 항, 및 제 75 항 중 한 항에 있어서,

사용자의 비밀키를 구하기 위한 상기 수단이 상기 사용자의 휴대용 메모리로부터 상기 사용자 비밀키를 판독하기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 102

제 28 항 또는 제 29 항에 있어서,

상기 비밀키를 구하기 위한 상기 수단이 상기 사용자의 휴대용 메모리로부터 상기 사용자의 비밀키를 판독하기 위한 수단을 구비하는 것을 특징으로 하는 시스템.

청구항 103

제 10 항, 제 11 항, 제 19 항, 제 21 항, 제 22 항, 및 제 55 항 중 한 항에 있어서,

상기 애플리케이션 패키지가 패키지 매체상에 기록되는 것을 특징으로 하는 방법.

청구항 104

제 103 항에 있어서,

상기 패키지 매체가 1회-기록형이고, 상기 클라이언트가 상기 1회-기록형의 상기 패키지 매체를 플레이할 수 있는 시스템인 것을 특징으로 하는 방법.

청구항 105

제 28 항, 제 29 항, 제 37 항, 제 39 항, 제 40 항, 제 70 항, 및 제 88 항 중 어느 한 항에 있어서,

상기 애플리케이션 패키지가 패키지 매체상에 기록되는 것을 특징으로 하는 시스템.

청구항 106

제 105 항에 있어서,

상기 애플리케이션 패키지가 1회-기록형의 패키지 매체상에 기록되는 것을 특징으로 하는 시스템.

청구항 107

제 105 항에 있어서,

상기 패키지 매체를 제작한 이후에, 상기 볼륨 제어 데이터의 적어도 일부가 상기 적어도 한 애플리케이션이 기록되는 데이터 영역과 다른 영역에 기록되는 것을 특징으로 하는 시스템.

청구항 108

제 107 항에 있어서,

상기 클라이언트가 상기 1회-기록형의 상기 패키지 매체를 플레이하기 위한 수단을 갖춘 시스템인 것을 특징으로 하는 시스템.

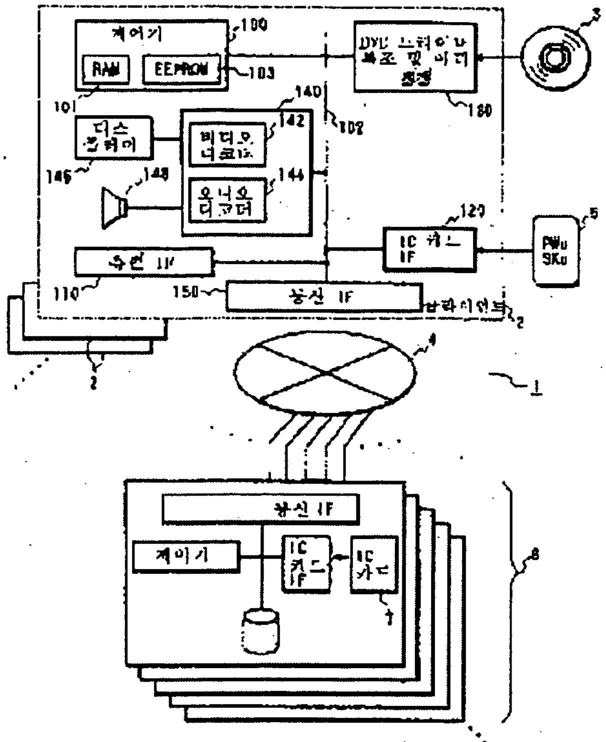
청구항 109

제 28 항, 제 29 항, 제 37 항, 제 39 항, 제 40 항, 제 70 항, 및 제 88 항 중 한 항에 있어서,

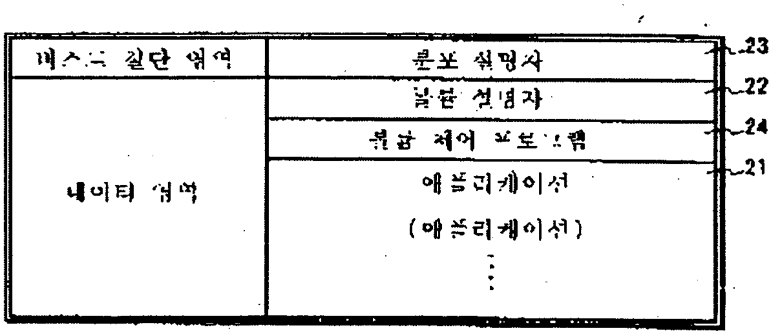
상기 애플리케이션 패키지가 DVD상에 기록되고, 상기 볼륨 제어 데이터의 적어도 일부가 상기 패키지 매체를 제작한 이후에 DVD의 BCA(burst cutting area)에 기록되고, 여기서 상기 클라이언트는 상기 DVD를 플레이하기 위한 수단을 갖춘 시스템인 것을 특징으로 하는 시스템.

도면

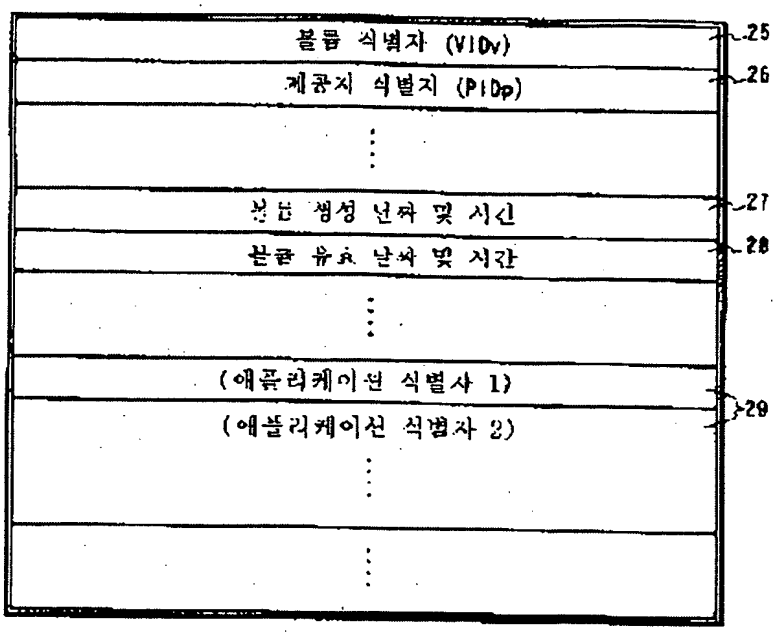
도면1


제어기
100
RAM
EEPROM
103
101
140
142
102
180
3
146
148
144
120
5
IC 카드 IF
PWu
SKu
110
150
통신 IF
2
4
1
통신 IF
제어기
IC 카드
7
8

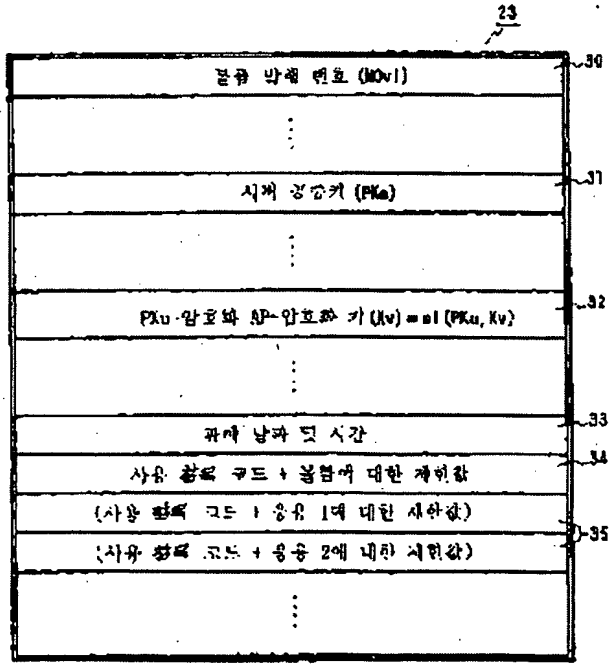
도면2


23
22
24
21
데이터 영역
애플리케이션
(애플리케이션)

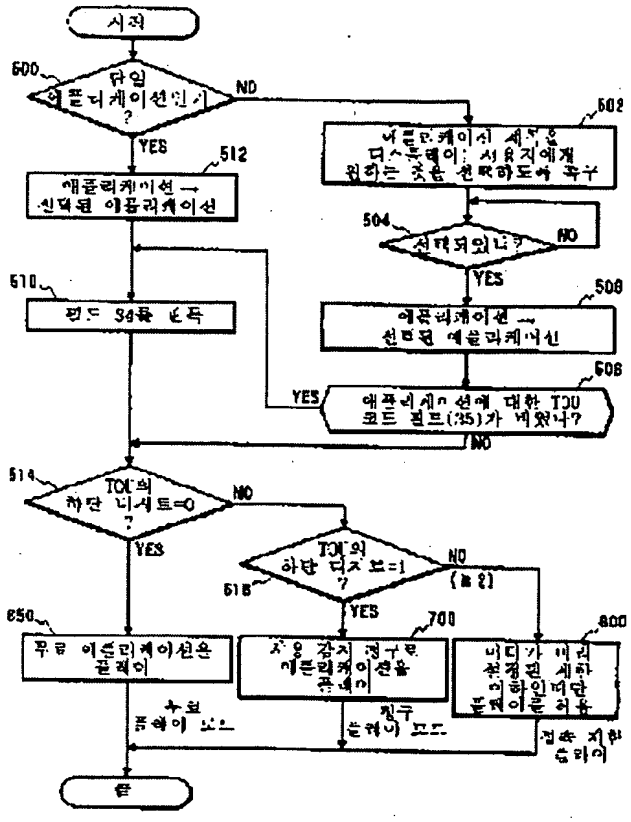
도면3


볼륨 식별자 (VIDv)
25
제공지 식별지 (PIDp)
26
27
28
29
(애플리케이션 식별자 1)
(애플리케이션 식별자 2)

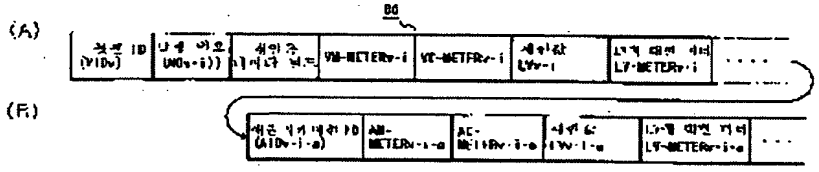
도면4


23
30
31
32
33
34
35

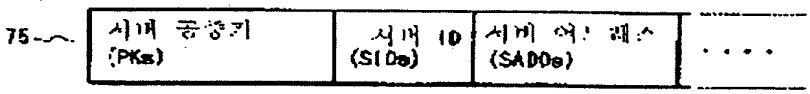
도면5


시작
600
타임 애플리케이션인가?
ND
YES
512
애플리케이션 → 선택된 어플리케이션
502
어플리케이션 제공업 디스플레이: 사용자에게 원하는 것을 선택하도록 촉구
504
선택되었나?
NO
YES
508
애플리케이션 → 선택된 애플리케이션
510
헤드 정보를 추출
506
YES
애플리케이션에 대한 TOU 코드 필드(35)가 비었나?
NO
514
TOU의 하단 니블=0 ?
NO
YES
516
TOU의 하단 니블=1 ?
NO
YES
850
무료 어플리케이션을 플레이
700
사용 감지 전구로 어플리케이션을 플레이
800
비디오 게임 분절된 세하 어플리케이션을 플레이
무료 플레이 모드
친구 플레이 모드
접속 지원 플레이
끝

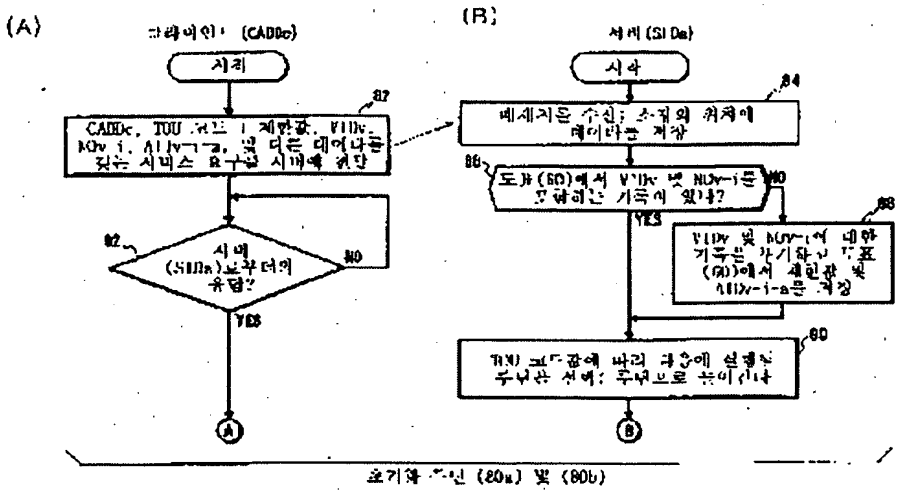
도면6


(A)
(F)
80

도면7


75
시계 공장키 (PKs)
시계 ID (SIDs)
시계 어드레스 (SADDs)

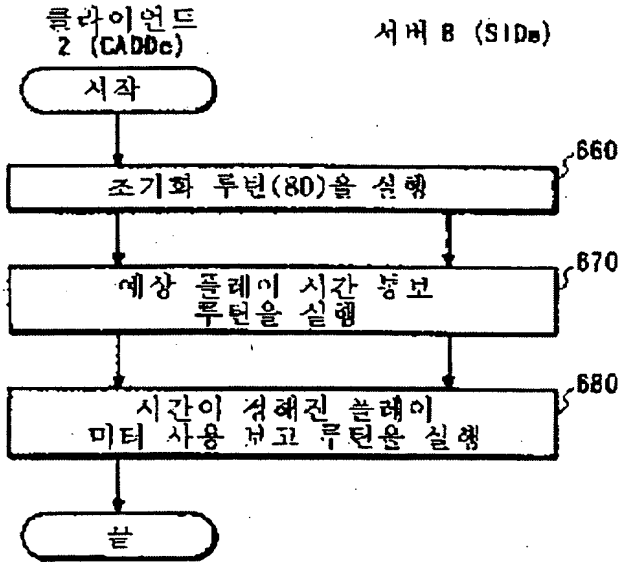
도면8



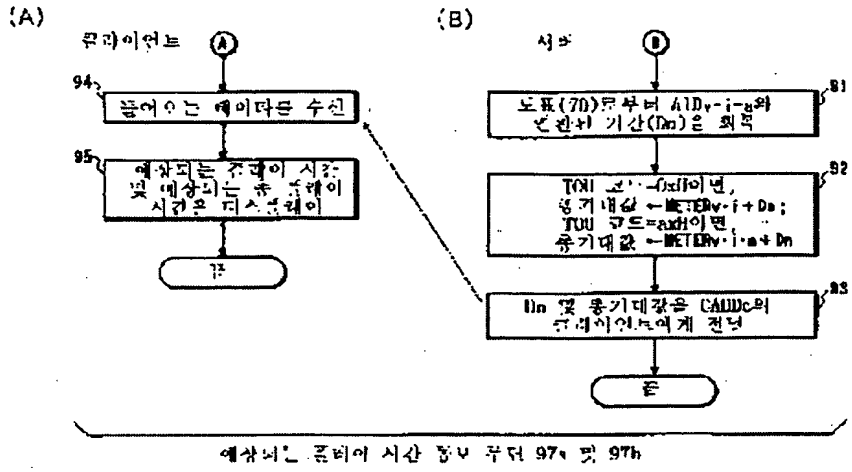
도면9

무료 애플리케이션을 플레이

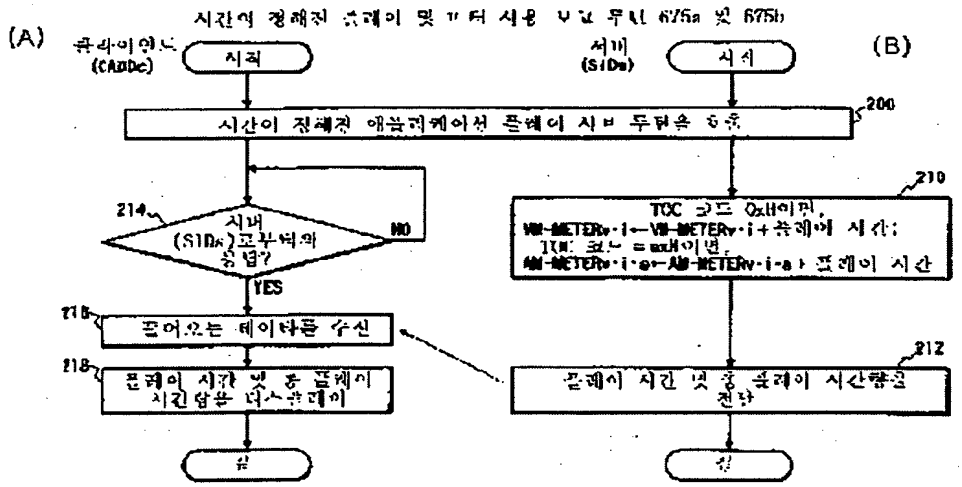
650



도면10



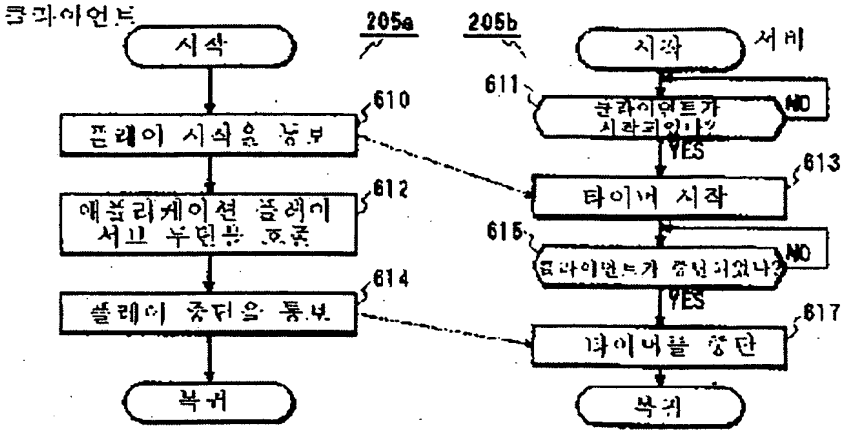
도면11



도면12

【A】 【B】

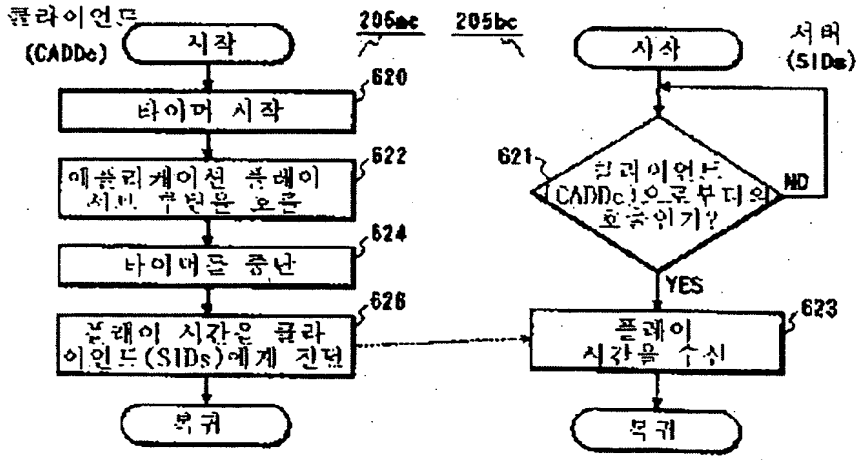
시간이 정해진 애플리케이션 플레이 서브 루틴



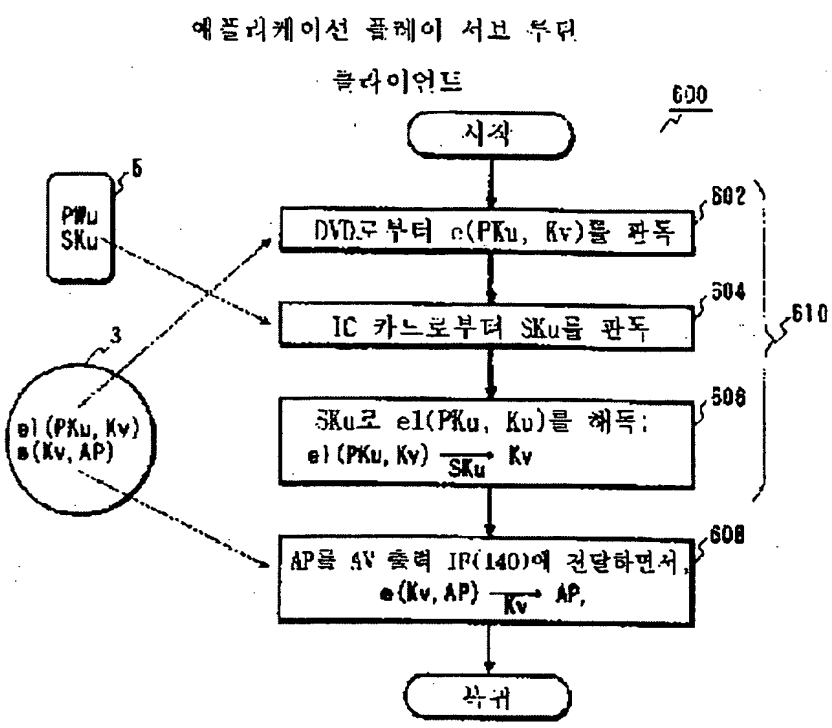
도면13

【A】 【B】

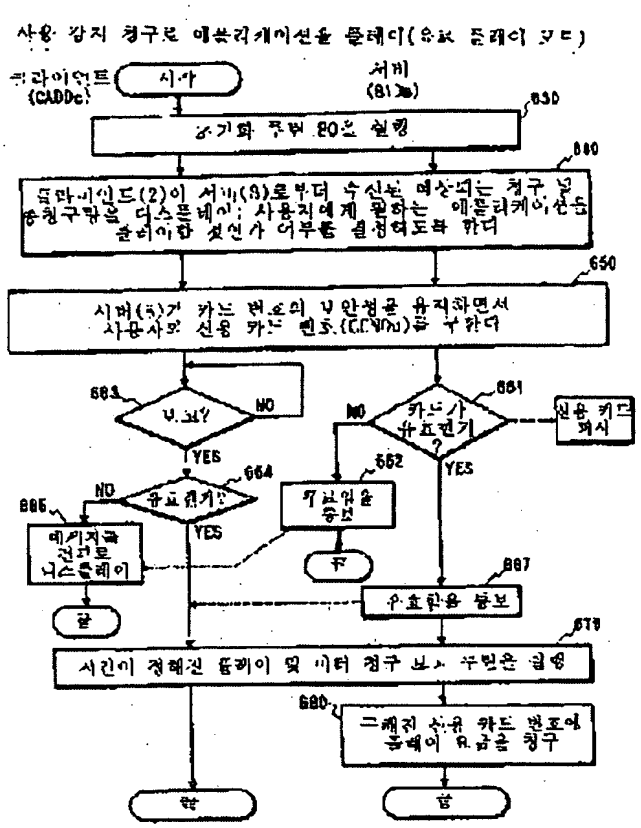
시간이 정해진 애플리케이션 플레이 서버 루틴



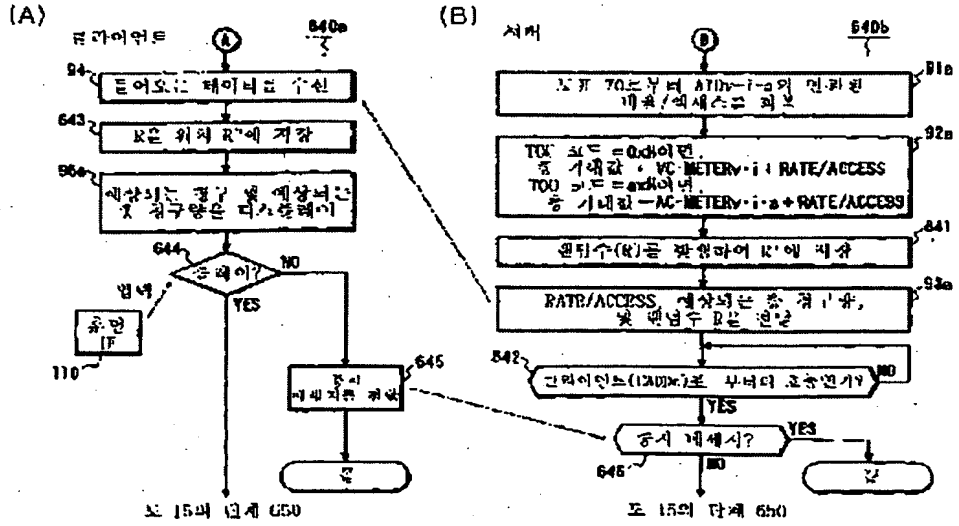
도면14


애플리케이션 플레이 서브 루틴
플라이언드
600
시작
5
PKu
SKu
3
e1(PKu, Kv)
e(Kv, AP)
DVD로부터 e(PKu, Kv)를 판독
602
IC 카드로부터 SKu를 판독
604
610
SKu로 e1(PKu, Ku)를 해독;
e1(PKu, Kv) SKu Kv
606
AP를 AV 출력 IP(140)에 전달하면서,
e(Kv, AP) Kv AP,
608
복귀

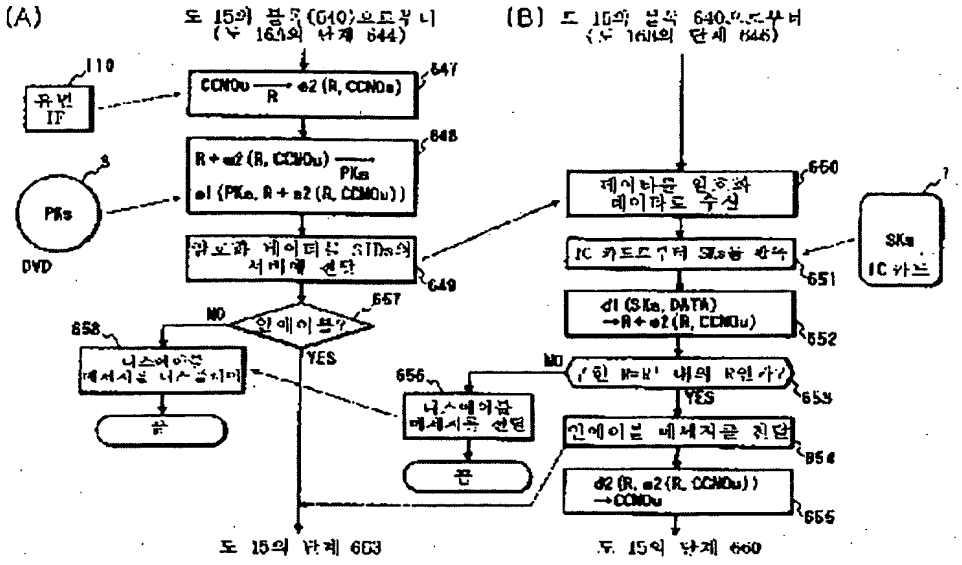
도면15


사용 장치 정구로 애플리케이션을 플레이(유료 플레이 모드)
클라이언트 (CADDc)
시작
서버 (BIDs)
630
초기화 루틴 80을 실행
640
650
NO
YES
661
662
664
666
667
679
680
끝

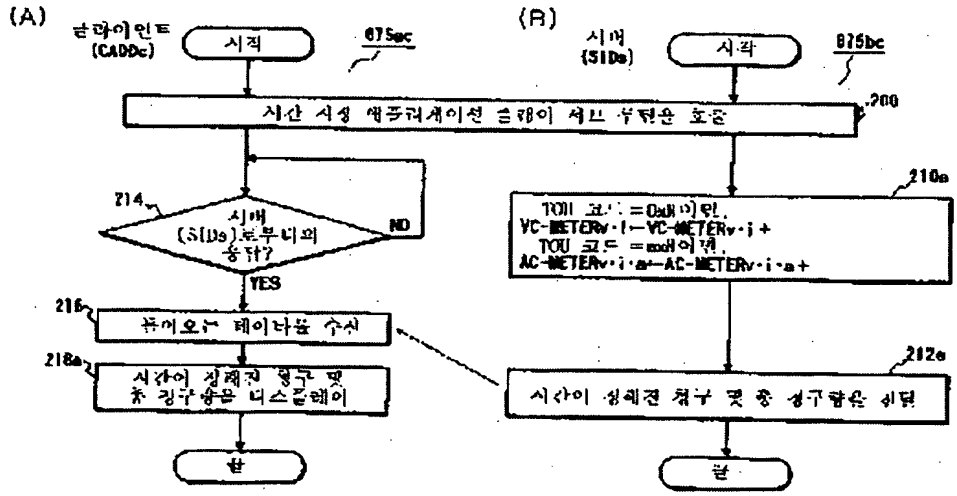
도면16


(A)
(B)
640a
640b
644
645
646
110
91a
92a
93a
841
842
YES
NO

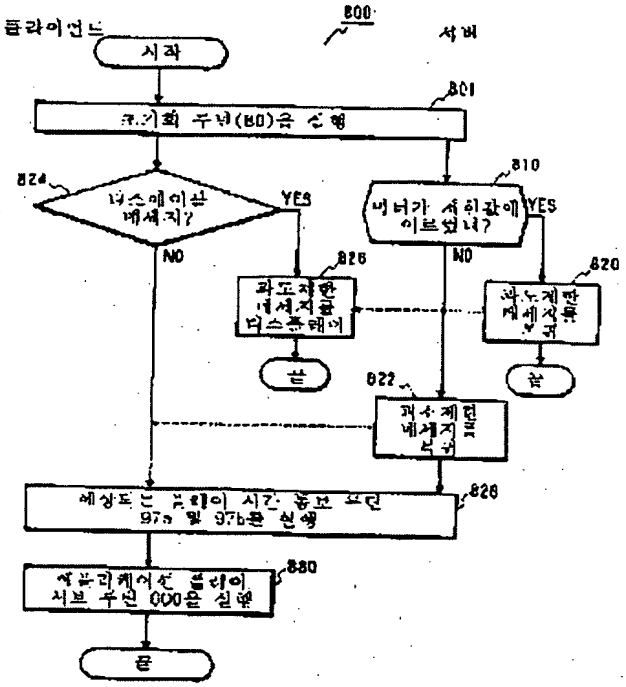
도면17


(A)
도 15의 블록(640)으로부터
(도 16A의 단계 644)
110
유선 IF
647
CCNOu → e2 (R, CCNOu)
R
648
R + e2 (R, CCNOu) → PKs
e1 (PKs, R + e2 (R, CCNOu))
S
PKs
DVD
649
암호화 데이터를 SIDs의 처리에 전달
657
인에이블?
NO
YES
658
디스에이블 메세지를 디스플레이
656
디스에이블 메세지를 전달
끝
끝
도 15의 단계 603
(B)
도 15의 블록 640으로부터
(도 16A의 단계 646)
660
데이타를 암호화 데이타로 수신
7
SKs
IC 카드
IC 카드로부터 SKs를 판독
651
d1 (SKs, DATA)
→R + e2 (R, CCNOu)
652
(R=R' 인가?)
NO
YES
653
인에이블 메세지를 전달
654
d2 (R, e2 (R, CCNOu))
→CCNOu
655
도 15의 단계 660

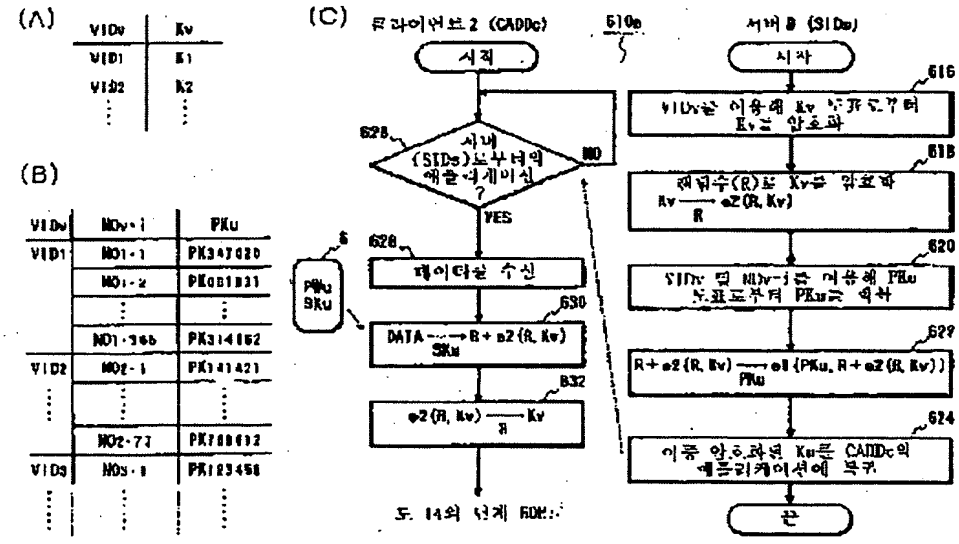
도면18


(A)
클라이언트 (CADDc)
시작
675ac
시간 서명 캘리브레이션 클럭이 서브 루틴을 호출
200
214
시버 (SIDs)로부터의 응답?
NO
YES
216
유에오누 데이타를 수신
218a
시간이 정해진 청구 및 추 청구항을 디스플레이
끝
(B)
시버 (SIDs)
시작
675bc
210a
TOU 코드 = 0a이면,
VC-METERv·i←VC-METERv·i+
TOU 코드 = ma이면,
AC-METERv·i·a←AC-METERv·i·a+
212a
시간이 정해진 청구 및 청구항을 저장
끝

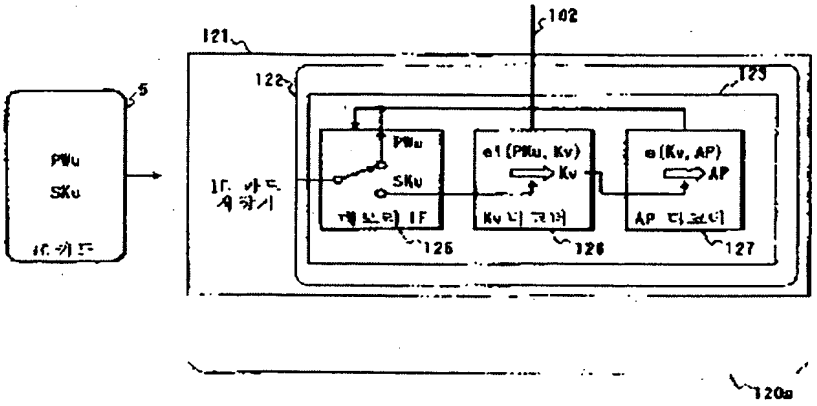
도면19


클라이언트
800
서버
시작
801
초기화 루틴(BD)을 실행
824
디스에이블 메세지?
YES
NO
810
버퍼가 저하값에 이르렀나?
YES
NO
826
과도적한 메세지를 디스플레이
820
파노계판 메세지들 무시
끝
822
과수제한 메세지 보냄
828
세상도는 프레임 시간 동보 프로그램 97a 및 97b를 실행
880
애플리케이션 클라이언트 루틴 600을 실행
끝

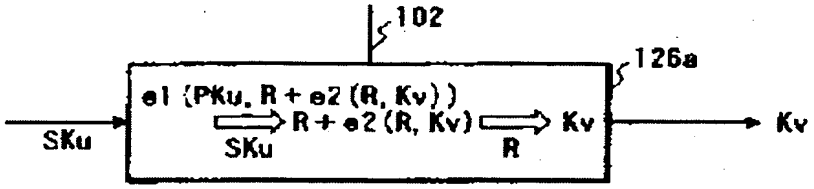
도면20


(A)
VIDv
Kv
VID1
K1
VID2
K2
(B)
VIDv
NOv-i
PKu
VID1
NO1-1
PK347020
NO1-2
PK081831
NO1-365
PK314162
VID2
NO2-1
PK141421
NO2-77
PK788612
VIDs
NOs-1
PK123456
(C)
클라이언트 2 (CADDc)
510b
서버 B (SIDs)
시작
시작
616
VIDv를 이용해 Kv 데이터베이스에서 Kv를 검색
618
랜덤수(R)로 Kv를 암호화
R
620
SIDv 및 NOv-i를 이용해 PKu 데이터베이스로부터 PKu를 검색
622
R+e2(R, Kv) PKu e1(PKu, R+e2(R, Kv))
624
이중 암호화된 Ku를 CADDc의 애플리케이션에 복구
끝
628
서버 (SIDs)로부터의 메세지인가?
NO
YES
6
PKu SKu
626
데이터를 수신
630
DATA SKu R+e2(R, Kv)
632
e2(R, Kv) R Kv
도 14의 단계 608로

도면21


121
102
122
123
5
PKu
SKu
PKu
SKu
e1 (PKu, Kv)
Kv
e (Kv, AP)
AP
125
126
127
120a

도면22


102
126a
e1 (PKu, R + e2 (R, Kv))
SKu
R + e2 (R, Kv)
SKu
Kv
R
Kv

도면23

사용 정책 코드의 상단 디지트(16진수)	사용 정책 코드가 저장되는 위치
0	전체 필름
1	애플리케이션 1
2	애플리케이션 2
⋮	⋮

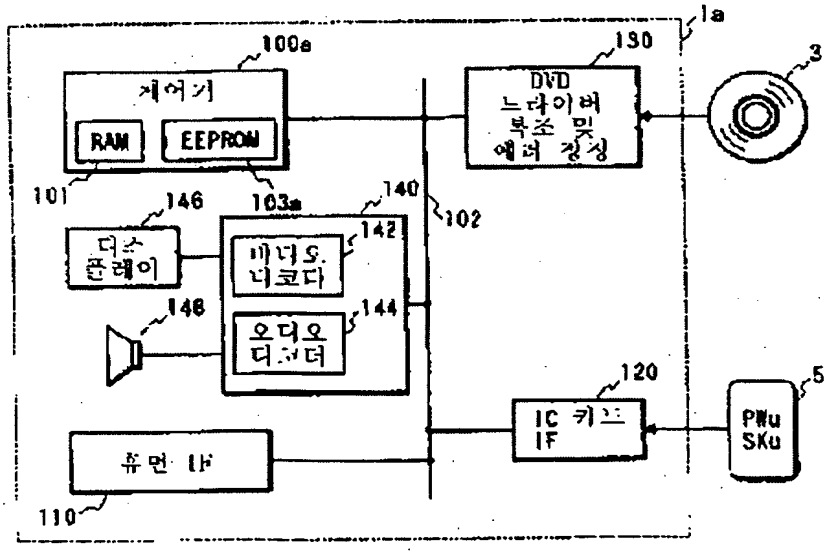
38

XY(X, Y = 1, 2, ···, F)

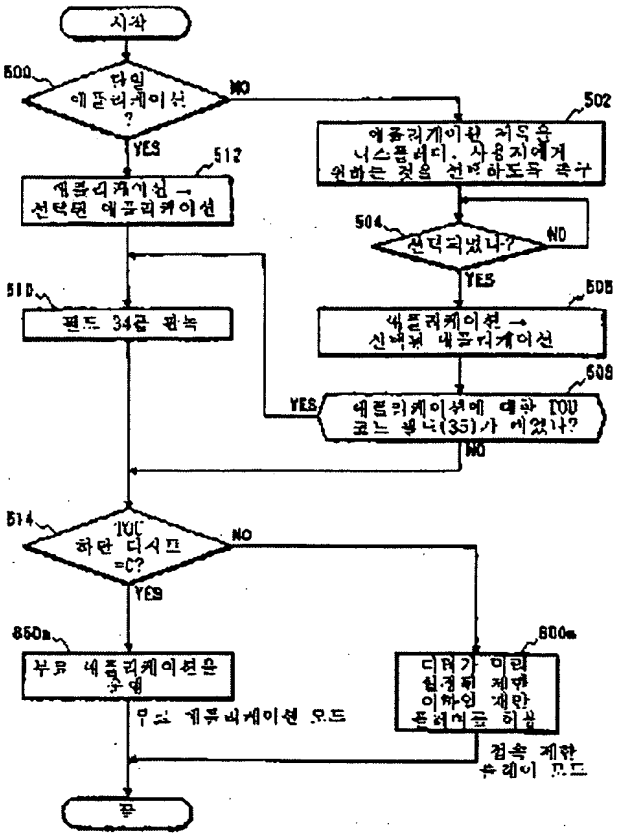
사용 정책 코드의 상단 디지트(16진수)	사용하는 제한값
0	없음 (무효)
1	없음 (유효)
2	유효 날짜 및 시간
3	허용 가능한 만기 날짜 및 시간
4	사용 주기의 최대값
5	허용가능한 이세스 카운트
⋮	⋮

37

도면24

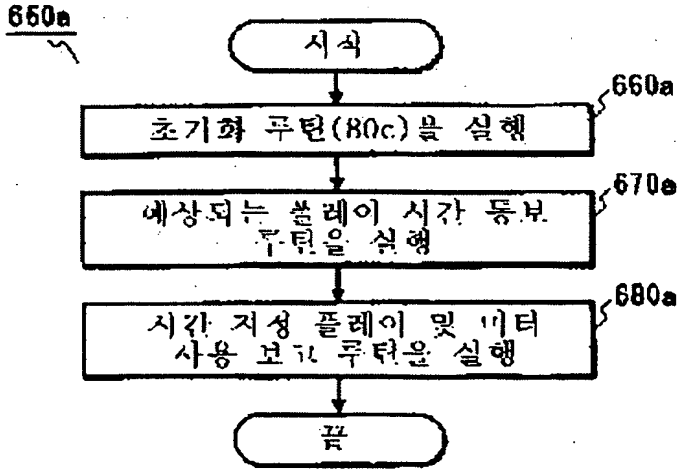


도면25

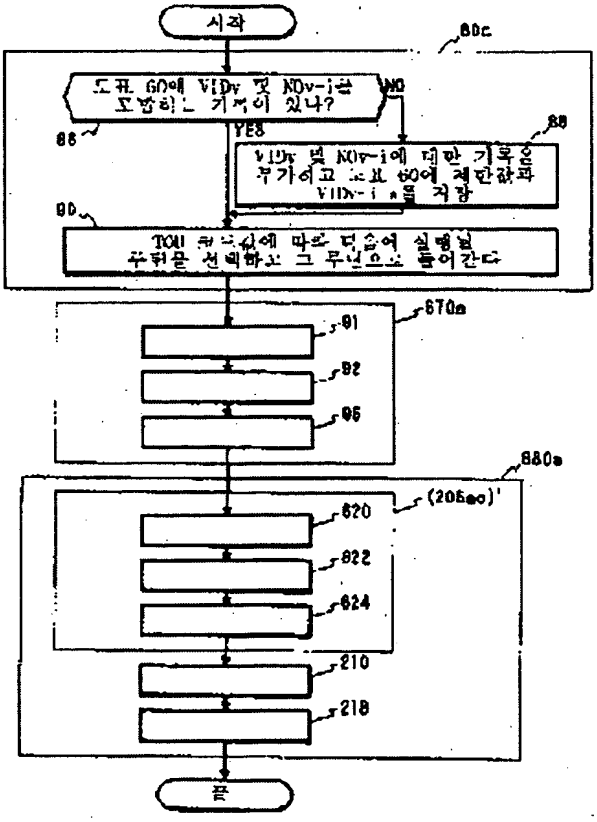


도면28

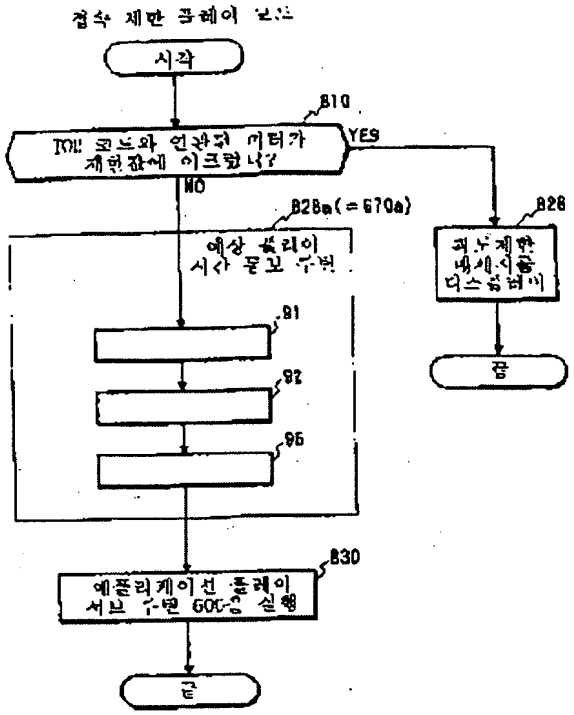
부분 플레이 모드



도면27


시작
80c
도표 60에 VIDv 및 MDv-i를
포함하는 기록이 있나?
NO
YES
86
88
VIDv 및 MDv-i에 대한 기록을
부가하고 도표 60에 제한값과
VIDv-i 값을 저장
90
TOM 코드값에 따른 다음에 실행될
루틴을 선택하고 그 루틴으로 들어간다
870a
91
92
95
880a
(205aa)'
820
822
824
210
218
끝

도면28


접속 제한 플레이 모드
시작
B10
TOL 코드와 인증된 데이터가 재현장에 있습니까?
YES
NO
B28a(=670a)
예상 플레이 시간 묘사 루틴
B28
괴수제한 네세이홀 디스플레이
B1
B2
B5
B30
에플리케이션 플레이 서브 루틴 600을 실행
끝
끝